

---

15 de Mayo de 2009

# CPS IPS.v3.1 Rev.00

---

**CPS de IPS CERTIFICATION  
AUTHORITY**

---

**IPS CERTIFICATION AUTHORITY, S.L.**

**Edificio Twin Golf A**

**C/Perú, 6**

**28290 - Las Rozas**

**Madrid (España)**

**Tel. + 34 916 308 568**

**Fax + 34 917 710 757**

**general@ipsca.com**

**http://www.ipsca.com**



CPS de IPS CERTIFICATION AUTHORITY

CPS

Versión 3.1

Fecha de Publicación: MAYO de 2009

CPS de IPS CERTIFICATION AUTHORITY

□ 2009, 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 IPS CERTIFICATION AUTHORITY.

**IPS Certification Authority, S.L. (IPS CERTIFICATION AUTHORITY)**

**CIF B60929452**

**Edificio Twin Golf A**

**C/Perú, 6**

**28290 - Las Rozas**

**Madrid (España)**

**Tel. + 34 916 308 568**

**Fax + 34 917 710 757**

**general@ipsca.com**

---

Resumen del  
CPS de IPS CERTIFICATION  
AUTHORITY

---

**IPS CERTIFICATION AUTHORITY**

Edificio Twin Golf A

C/Perú, 6

28290 - Las Rozas

Madrid (España)

Tel. + 34 916 308 568

Fax + 34 917 710 757

[general@ipsca.com](mailto:general@ipsca.com)

<http://www.ipsca.com>

**IPS CERTIFICATION AUTHORITY, Práctica Profesional de Certificación (CPS),****resumen:****Garantía**

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

IPS CERTIFICATION AUTHORITY también garantiza que cualquier certificado es revocado si en cualquier momento IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY realiza para verificar la información contenida en un certificado varía según los gastos de certificación cobrados, la naturaleza e identidad del suscriptor del certificado, y por los documentos que permiten que el certificado sea catalogado como “de confianza”. En todo caso los trámites efectuados por IPS CERTIFICATION AUTHORITY serán suficientes a los efectos de esta garantía. IPS CERTIFICATION AUTHORITY no da otras garantías.

**Responsabilidad**

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

**Confidencialidad**

Los contenidos de los certificados emitidos por IPS CERTIFICATION AUTHORITY son información pública. IPS CERTIFICATION AUTHORITY se obliga a no divulgar 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**

IPS CERTIFICATION AUTHORITY no acepta ninguna responsabilidad por cualquier falta de cumplimiento de la garantía, retraso o no cumplimiento de la 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**

IPS CERTIFICATION AUTHORITY podrá revocar o suspender certificados a su sola discreción, y publicará la lista de certificados revocados en una Lista de Certificados Revocados que sea pública y accesible.

### **Mantenimiento de Datos**

IPS CERTIFICATION AUTHORITY mantendrá los datos y documentos relativos a la emisión de certificados por un plazo mínimo de 5 años, sin perjuicio del ejercicio del derecho de cancelación sobre los datos de carácter personal.

### **Contenido del Certificado**

Cada certificado emitido por IPS CERTIFICATION AUTHORITY tiene por objeto el certificar únicamente la información contenida en el mismo. IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY o frente a terceros de cualquier declaración incorrecta que hayan hecho a IPS CERTIFICATION AUTHORITY, 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 IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY 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 en el certificado por referencia, así como los contenidos de esta Práctica Profesional de Certificación y la Lista de Certificados Revocados publicada por IPS CERTIFICATION AUTHORITY.

### **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 IPS CERTIFICATION AUTHORITY, el reclamante debe notificar a IPS CERTIFICATION AUTHORITY por escrito y por correo certificado de la naturaleza exacta de la reclamación. El reclamante debe dejar un tiempo razonable a IPS CERTIFICATION AUTHORITY para permitir resolver la reclamación antes de invocar cualquier proceso de resolución de conflictos.

En el caso de que IPS CERTIFICATION AUTHORITY 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.

### **Autoridades de Certificación de Segundo Nivel:**

#### **Práctica y Responsabilidad**

IPS CERTIFICATION AUTHORITY puede delegar su confianza a otras Autoridades de Certificación mediante certificación en cadena o certificación cruzada.

IPS CERTIFICATION AUTHORITY requiere que estas Autoridades de Certificación verifiquen el contenido de un certificado con procesos que sean como mínimo tan seguros como los empleados por IPS CERTIFICATION AUTHORITY y que se detallan en el CPS de IPS CERTIFICATION AUTHORITY y de la Autoridad de Certificación de Segundo Nivel.

---

**Documento integro**  
**CPS de IPS CERTIFICATION**  
**AUTHORITY**

---

**IPS Certification Authority, S.L. (IPS  
CERTIFICATION AUTHORITY)**

**Edificio Twin Golf A**

**C/Perú, 6**

**28290 - Las Rozas**

**Madrid (España)**

**Tel. + 34 916 308 568**

**Fax + 34 917 710 757**

**general@ipsca.com**

**www.ips.es**

## 1 INTRODUCCIÓN

### 1.1 Presentación

IPS CERTIFICATION AUTHORITY, S.L. **ÚNICAMENTE**, emite Certificados para CA's de Segundo Nivel. La presente CPS, que incluye implícitamente la Norma de Certificación, establece las normas, políticas y procedimientos para la emisión de estos Certificados y los Certificados que pudieran emitir la CA' s de Segundo Nivel Certificadas por IPS CERTIFICATION AUTHORITY, S.L., aunque ésta **NO EMITA DIRECTAMENTE** estos últimos tipos de Certificados.

El presente documento constituye la CPS de IPS CERTIFICATION AUTHORITY, donde se definen los mecanismos relacionados con la práctica de certificación de IPS CERTIFICATION AUTHORITY. Asimismo, en la presente CPS se recoge **IMPLÍCITAMENTE** la Norma de Certificación que IPS CERTIFICATION AUTHORITY, S.L. observa en la emisión de Certificados. Esta Declaración de Prácticas de Certificación (CPS) de IPS CERTIFICATION AUTHORITY está basada en la propuesta del IETF PKIX, de S. Chokhani y W. Ford.

La presente CPS presenta las prácticas que IPS CERTIFICATION AUTHORITY y, cuando así se recoja expresamente en este CPS, las CA's de Segundo Nivel con Certificados de IPS CERTIFICATION AUTHORITY, 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. La CPS abarca 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 la prestación de servicios de certificación. Las partes que actúan en la prestación de servicios de certificación de IPS CERTIFICATION AUTHORITY están ligadas a sus obligaciones en virtud de sus contratos con IPS CERTIFICATION AUTHORITY.

### 1.2. Estructura

La CPS regula el de ciclo de vida del certificado y describe el proceso de certificación. La estructura de esta 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 Certificados para CA de Segundo Nivel.

### **1.6 Certificados que podrán emitir las CA de Segundo Nivel**

1.6.1 B1. Certificados de Correo con validez mensual/anual.

1.6.2 B2. Certificado Personal con verificación documental.

1.6.3 B3. Certificado Personal Presencial.

1.6.4 B4. Certificado Personal Presencial ante Fedatario Público.

1.6.5 A1. Certificados de Servidor.

### **1.7 Limitación en el uso de los Certificados.**

### **1.8 Detalles de contacto.**

## **2 ASPECTOS GENERALES.**

### **2.1 Obligaciones.**

2.1.1 Obligaciones de IPS CERTIFICATION AUTHORITY.

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 IPS CERTIFICATION AUTHORITY.****2.4 Interpretación y ejecución.**

- 2.4.1 Ley aplicable.
- 2.4.2 Notificaciones en el caso de escisión, supervivencia y fusión.
- 2.4.3 Procedimiento de resolución de conflictos.
- 2.4.4 Tasas de registro por la expedición y revocación de Certificados.

Política de Reembolso.

**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.****2.8 Auditoría.**

- 2.8.1 Auditorías Internas.
- 2.8.2 Auditorías Externas.

**3 IDENTIFICACIÓN Y AUTENTICACIÓN. GENERACIÓN DE CERTIFICADOS.****3.1 Certificados para CA de Segundo Nivel.****3.2 Certificados que podrán emitir las CA de Segundo Nivel.**

- 3.2.1 B1. Certificados de Correo con validez mensual/anual.
- 3.2.2 B2. Certificado Personal con verificación documental.
- 3.2.3 B3. Certificado Personal Presencial.
- 3.2.4 B4. Certificado Personal Presencial ante Fedatario Público.
- 3.2.5 A1. Certificados de Servidor.
- 3.2.6 A1. Certificados de Servidor (Previo Acuerdo).

**4 GESTIÓN DE LAS CLAVES.****4.1 Aspectos Generales.****4.2 Gestión de las claves de la CA.****4.3 Gestión de las claves del solicitante/suscriptor.**

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

### **5.1 Supuestos de la revocación.**

5.1.1 Efectos de la revocación.

### **5.2 Supuestos de la suspensión.**

5.2.1 Efectos y límites de la suspensión.

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

5.3.1 Legitimación activa.

5.3.2 Recepción de solicitudes de suspensión/revocación.

5.3.3 Decisión de suspender/revocar.

5.3.4 Comunicación y publicación de la suspensión/revocación.

## **6 CADUCIDAD DE CERTIFICADOS.**

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

### **7.1 Renovación de Certificados.**

7.1.1 Requisitos previos.

7.1.2 Cómo solicitar la renovación.

7.1.3 Procedimiento de renovación de Certificados.

### **7.2 Reemisión de Certificados.**

7.2.1 Requisitos previos.

7.2.2 Cómo solicitar la reemisión.

7.2.3 Procedimiento de reemisión de Certificados.

### **7.3 Regeneración de claves**

## **8 EXTINCIÓN DE LA CA.**

## **9 CONTROLES DE SEGURIDAD.**

### **9.1 Manual Interno de Seguridad.**

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

### **9.3 Seguridad del Personal.**

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

### **9.5 Seguridad en la gestión de sistemas.**

### **9.6 Seguridad para usuarios de sistemas.**

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

### **9.8 Incidencias.**

### **9.9 Cumplimiento.**

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

**10.1 Características del Certificado.**

**10.2 Listas de Certificados.**

**10.3 Consulta de estado de Certificados o revocación on line**

## **11 OTRAS CUESTIONES.**

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

**11.2 Procedimiento de publicación de las modificaciones.**

**11.3 Procedimiento de notificación de las publicaciones.**

### **1.3 Identificación**

Esta CPS puede ser consultada por Internet en el servidor web de IPS CERTIFICATION AUTHORITY, [www.ips.es](http://www.ips.es), o personalmente en las oficinas de IPS CERTIFICATION AUTHORITY.

Todos los solicitantes y suscriptores de certificados manifiestan que conocen este documento, antes de la petición de cualquier tipo de certificado a IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY,

**IPS Certification Authority, S.L. (IPS  
CERTIFICATION AUTHORITY)****CIF B60929452**

**Edificio Twin Golf A**  
**C/Perú, 6**  
**28290 - Las Rozas**  
**Madrid (España)**  
**Tel. + 34 916 308 568**  
**Fax + 34 917 710 757**  
**general@ipsca.com**

**1.4 Comunidad de usuarios y aplicabilidad**

La presente CPS **se aplica** a todos los Certificados emitidos por IPS CERTIFICATION AUTHORITY, S.L.. IPS CERTIFICATION AUTHORITY sólo emite Certificados encadenados para otras CA's subordinadas. Las Prácticas recogidas en la presente CPS, que a su vez, recoge implícitamente las Normas de Certificación, se aplica a la emisión y uso de Certificados emitidos por IPS CERTIFICATION AUTHORITY, S.L., así como a la CRL de Certificados de IPS CERTIFICATION AUTHORITY, S.L, además de a las CA's subordinadas a las que se han emitido Certificados de IPS CERTIFICATION AUTHORITY, S.L.

**1.4.1 Autoridad de Certificación**

IPS CERTIFICATION AUTHORITY actúa como Autoridad de Certificación 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.

**1.4.2 Autoridad de Registro**

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

IPS CERTIFICATION AUTHORITY 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. En su caso, la relación con las Autoridades de Registro deberá regirse por contratos específicos de prestación de servicios.

IPS CERTIFICATION AUTHORITY no prevé en la utilización de AR para verificar las identidades de las CA's de Segundo Nivel. Por esta razón en el presente CPS no se establecen las normas que deben cumplir las AR con respecto a la validación de la identidad de la AR o de la autenticidad de las peticiones de solicitud de certificados recibidas de AR externas

#### **1.4.3 Suscriptor**

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. Únicamente podrán ser suscriptores de Certificados para Certificados para CA de Segundo Nivel personas jurídicas.

#### **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 PRÁCTICAS DE CERTIFICACIÓN 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 la Autoridad Certificadora.

Cuando el Usuario decida voluntariamente confiar y hacer uso del Certificado le será de aplicación la presente CPS.

### **1.5 Tipos de Certificados**

IPS CERTIFICATION AUTHORITY, S.L. **ÚNICAMENTE**, emite Certificados para CA's de Segundo Nivel. El presente apartado establece, además de los Certificados para CA's de Segundo Nivel, otros Certificados que pudieran emitir la CA' s de Segundo Nivel Certificadas por IPS CERTIFICATION AUTHORITY,

S.L., aunque ésta **NO EMITA DIRECTAMENTE** este último tipo de Certificados.

#### **1.5.1.Certificados para CA de Segundo Nivel:**

Los Certificados para CA de Segundo Nivel, son aquellos Certificados para una CA Encadenada, es decir, aquella CA donde sus certificados forman parte de la jerarquía de certificados de IPS CERTIFICATION AUTHORITY, por lo que son reconocidos técnicamente de forma nativa por los programas de correo, navegadores y servidores web. Las CA de Segundo Nivel se rigen por lo estipulado en esta CPS y además deben cumplir con compromisos técnicos de seguridad y gestión. Una CA Corporativa se establece mediante un contrato, incluso ante notario en cuanto al cumplimiento de estos compromisos.

**1.6. Certificados que podrán emitir las CA de Segundo Nivel:**

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

**1.6.1. 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.

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

**1.6.2. B2. Certificado Personal con verificación documental**

Es necesaria la comprobación de la identidad del sujeto mediante un documento de identidad válido. Deberá enviarse una fotocopia del documento.

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.

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

### **1.6.3. B3. Certificado Personal Presencial.**

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

Los certificados de Categoría B3 son empleados por los suscriptores para garantizar frente a terceros su identidad, la autenticidad y la integridad de sus mensajes, en Intranet o Internet, en particular mediante la utilización de aplicaciones de correo electrónico seguro S/MIME, para cifrar y firmar mensajes, con un nivel de autenticación superior a la Categoría 1, resultando idóneos para su empleo en el ámbito de la Administración en general.

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 de Registro correspondientes, gozando estos certificados de la naturaleza jurídica de documento oficial. Los documentos firmados son, en todo caso, documentos privados.

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

### **1.6.4. B4. Certificado Personal Presencial ante Fedatario Público**

La comprobación de la persona será presencial y documental ante un fedatario público. El individuo deberá presentarse ante el registrador (fedatario público) con un documento de identidad válido.

Los certificados B4 son empleados por los suscriptores para garantizar frente a terceros su identidad, la autenticidad y la integridad de sus mensajes, en Intranet o Internet, en particular mediante la utilización de aplicaciones de correo electrónico seguro S/MIME, para cifrar y firmar mensajes, cuando la Ley exija la intervención de fedatario público en la transacción. Suponen el mayor nivel posible de autenticación previa del suscriptor del certificado.

Todos los datos contenidos en el certificado se protocolizan de acuerdo con la normativa del fedatario público aplicable, gozando estos certificados de la naturaleza jurídica de documentos público. Los documentos firmados son, en todo caso, documentos privados.

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

#### **1.6.5. 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 el reconocimiento de la identidad de la empresa solicitante, 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.

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY. Se recoge en la presente CPS por ser de obligado cumplimiento para las CA's de Segundo Nivel.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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, el orden público y la moral.

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.

## **1.8. Detalles de contacto**

**Versión del CPS: 3.1**

**Fecha: 15 de mayo del 2009**

(En el presente CPS se recogen IMPLÍCITAMENTE las Normas de Certificación que IPS CERTIFICATION AUTHORITY, S.L. observa en la emisión de Certificados)

**IPS Certification Authority, S.L. (IPS CERTIFICATION  
AUTHORITY)  
CIF B60929452**

**Persona de Contacto: Rodolfo Lomascolo Szittyay  
Cargo: Director General**

**Edificio Twin Golf A  
C/Perú, 6  
28290 - Las Rozas  
Madrid (España)  
Tel. + 34 916 308 568  
Fax + 34 917 710 757  
[general@ipsca.com](mailto:general@ipsca.com)**

## **2. ASPECTOS GENERALES**

### **2.1 Obligaciones**

#### **2.1.1 Obligaciones de IPS CERTIFICATION AUTHORITY**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY

- 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 [www.ips.es](http://www.ips.es) toda la información necesaria.
- Publicar los certificados emitidos.
- Proteger los datos personales según requerimientos de la LOPD
- Cumplir las obligaciones de la presente CPS.
- Notificar la emisión de un Certificado a los suscriptores.
- Todas aquellas obligaciones impuestas por la presente CPS y, en su caso, el Real Decreto-Ley 14/1999, el Reglamento de firma electrónica, las leyes de protección de datos personales y por la normativa vigente.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La AR podrá asumir las siguientes obligaciones de las cuales será responsable. Según lo establecido con anterioridad, IPS CERTIFICATION AUTHORITY actúa como Autoridad de Registro

- 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.

- Validar las solicitudes de revocación y suspensión respecto a aquellos Certificados en cuya emisión hayan participado.
- 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 razonable la documentación aportada en el proceso de emisión del Certificado y en el proceso de suspensión/revocación del mismo.
- 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.

En todo caso, la AR permitirá a la CA 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 Prácticas de Certificación por parte de la AR o cualquier poseedor de un Certificado. La AR y los poseedores de cualquier Certificado deberán informar a la CA inmediatamente de cualquier sospecha de infracción.

La CA 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.

Todas las funciones atribuidas a las AR, siempre y cuando no exista colisión con los derechos reconocidos a éstas mediante acuerdos individuales, podrán ser desempeñadas de forma directa por parte de la CA, en cuyo caso toda referencia de esta CPS a una AR deberá entenderse hecha a la CA.

### **2.1.3 Obligaciones del Solicitante**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

- Abonar las tasas de registro que correspondan en virtud de los servicios que se soliciten.
- Solicitar el Certificado según se estipula en el CPS, las Prácticas de Certificación y en atención a las instrucciones de IPS CERTIFICATION AUTHORITY.
- Cualesquiera otras estipulaciones recogidas en el acuerdo suscrito entre él e IPS CERTIFICATION AUTHORITY.
- Ser veraz y exacto en la aportación de los datos solicitados.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

- 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.
- Solicitar la suspensión / revocación del Certificado cuando se cumpla alguno de los supuestos previstos en el epígrafe titulado "SUSPENSIÓN Y REVOCACIÓN DE CERTIFICADOS" de la presente CPS.
- No revelar la clave privada ni el código de activación del Certificado.
- Ser veraz y exacto en la aportación de los datos solicitados.
- Asegurarse de que toda la información contenida en el Certificado es cierta y notificar inmediatamente a la CA 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 la CA acerca de cualquier situación que pueda afectar a la validez del Certificado.

- Destruir el Certificado cuando así lo exija la CA 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 Prácticas de Certificación. 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 las PRACTICAS DE CERTIFICACIÓN o del acuerdo suscrito con IPS CERTIFICATION AUTHORITY.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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 CA no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.

Los usuarios de Certificados de IPS CERTIFICATION AUTHORITY tienen la obligación de conocer las limitaciones de uso que el Certificado pudiera contener. Además deberán aceptar el régimen de responsabilidad recogido en el apartado 2.2 del presente CPS.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un Certificado IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY con relación a las firmas emitidas mediante certificados por el 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**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

Toda persona tendrá derecho a confiar en un Certificado IPS CERTIFICATION AUTHORITY 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 IPS CERTIFICATION AUTHORITY con relación a las firmas emitidas mediante certificados por el 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 IPS CERTIFICATION AUTHORITY se obligan a conocer y aceptar los términos, condiciones y límites contenidos en esta CPS y en las PRACTICAS DE CERTIFICACIÓN específicas de su certificado, establecidas por contrato, dentro de los cuales se asegura la prestación de los servicios de certificación.

## **2.2 Responsabilidad**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA 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.

La CA no será responsable de la incorrecta utilización de los Certificados y las claves, ni de cualquier daño indirecto que pueda resultar de la utilización del Certificado o de la información suministrada por la CA. En particular, el lucro cesante, la pérdida de ingresos o pedidos o pérdida de datos tendrán la consideración de daños indirectos y los mismos no darán lugar a ningún tipo de derecho indemnizatorio.

La CA 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.

La CA 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 PRÁCTICAS DE CERTIFICACIÓN, incluidas implícitamente en el presente CPS, correspondientes a cada tipo de certificado.

La CA no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones en virtud del 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 la CA no pueda tener un control razonable y entre otros: los desastres naturales, la guerra, el estado de sitio, las alteraciones de orden público, la huelga en los transportes, el corte de suministro eléctrico y/o telefónico, los virus informáticos, deficiencias en los servicios de telecomunicaciones (Internet, Infovía Plus, Retenet, etc.) o el compromiso de las claves asimétricas derivado del riesgo tecnológico imprevisible.

La CA no será responsable del contenido de aquellos documentos firmados digitalmente ni de aquellas "páginas web" que contengan un certificado.

Cualquiera que sea la causa por la que pudiera reclamarse responsabilidad a la CA o la AR, la pretensión indemnizatoria no podrá exceder, salvo en el supuesto de culpa grave o dolo, la cantidad de 6.000 euros.

Los servicios de certificación de IPS CERTIFICATION AUTHORITY no han sido diseñados, destinados ni autorizados para su empleo como equipamiento de control en circunstancias peligrosas, nocivas, molestas e insalubres o para actividades que requieran funcionamiento a prueba de errores como sucede en instalaciones nucleares, navegación aérea o sistemas de comunicación, sistemas de control de

tráfico aéreo, o sistemas de control de armamento, en los que un error podría conducir a la muerte o lesiones de personas, o causar daños ambientales.

Ni IPS CERTIFICATION AUTHORITY 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.

No obstante a lo señalado en este apartado, anualmente IPS CERTIFICATION AUTHORITY, S.L. una evaluación de los riesgos de su labor certificadora e implementado los controles adecuados para minimizar los riesgos que se deriven de la mencionada evaluación.

IPS CERTIFICATION AUTHORITY y, en su caso, las AR, no son los Agentes, Fiduciarios ni Administradores o Representantes, en ningún caso, de los suscriptores, por lo que no asume ningún tipo de responsabilidad al respecto.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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 la CA.

### **2.2.3 Responsabilidad del Suscriptor**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el

término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

#### **2.2.4 Responsabilidad del Usuario**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

En todo caso, el Usuario asumirá toda la responsabilidad y riesgos derivados de la aceptación de un Certificado sin haber realizado previamente la preceptiva verificación de su validez, garantizando la plena indemnidad de la CA por dicho concepto.

#### **2.3 Usos de los Certificados IPS CERTIFICATION AUTHORITY**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

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 IPS CERTIFICATION AUTHORITY 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, se regirá por su legislación específica.

IPS CERTIFICATION AUTHORITY, S.L. no asume ninguna responsabilidad por el uso indebido o no autorizado de los Certificados.

## **2.4 Interpretación y ejecución**

### **2.4.1 Ley aplicable**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

El presente documento y las Prácticas de Certificación, que se recogen implícitamente en el CPS, específicas para cada tipo de Certificado se regirán por la Ley del Reino de España, con arreglo a la cual deberá ser interpretado su contenido.

### **2.4.2 Notificaciones en el caso de escisión, supervivencia y fusión:**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA 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, mediante correo electrónico, 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.

IPS CERTIFICATION AUTHORITY notificará de la forma prevista en el párrafo primero del presente apartado a los suscriptores y/o solicitantes de Certificados de

IPS CERTIFICATION AUTHORITY en los casos de escisión supervivencia y fusión.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Para la resolución de cualquier conflicto que pudiera surgir en relación a esta CPS o a las Prácticas de Certificación, recogidas implícitamente en el presente CPS, 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. Política de reembolso**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

Las tasas de registro vigentes en cada momento por la expedición y renovación de Certificados serán puestas a disposición de los Solicitantes a través de su publicación en el Servidor Web de IPS CERTIFICATION AUTHORITY, S.L o bajo petición a IPS CERTIFICATION AUTHORITY, S.L. En su caso, las AR podrán, dentro del área en el que presten sus servicios, establecer promociones especiales, ofertas o similares que modifiquen las tarifas previamente establecidas.

El acceso al Certificado, el acceso a la información del estado del Certificado y, en su caso, otros servicios relacionados con la labor Certificadora de IPS CERTIFICATION AUTHORITY, S.L., serán gratuitos.

No existe una Política de reembolso genérica, sino que dependerá de cada caso en concreto y será recogida, si es considerado necesario, en los acuerdos privados que

se suscriban entre IPS CERTIFICATION AUTHORITY, S.L. y los suscriptores de Certificados.

## **2.5 Publicación y depósito**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

El contenido de esta CPS, así como de toda la información que se publique, entendiéndose como tal la información sobre los certificados y la publicación periódica de las CRL, estará expuesta a título informativo en el servidor web: <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 IPS CERTIFICATION AUTHORITY.

No obstante lo señalado en el párrafo anterior, en el servidor web de IPS CERTIFICATION AUTHORITY, S.L. se encuentra disponible al público información sobre el CPS de IPS CERTIFICATION AUTHORITY, donde también se recoge implícitamente la Norma de Certificación que IPS CERTIFICATION AUTHORITY, S.L. observa en la emisión de Certificados, su política de precios, la política de privacidad, las condiciones de utilización del servidor web [www.ips.es](http://www.ips.es) y documentos asociados a la Ley Orgánica de Protección de Datos. La información señalada en este párrafo se caracteriza por su libre acceso.”

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

IPS CERTIFICATION AUTHORITY se obliga a guardar 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 IPS CERTIFICATION AUTHORITY proporcionan a sus clientes. Asimismo, una vez generadas y entregadas las claves privadas, IPS CERTIFICATION AUTHORITY se obliga a abstenerse 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**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

IPS CERTIFICATION AUTHORITY se obliga a mantener 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. IPS CERTIFICATION AUTHORITY se obliga a solicitar la autorización de Solicitantes y Suscriptores cuando precise utilizar los datos para otros fines.

### **2.6.3 Protección de datos**

Este apartado no se aplica a IPS CERTIFICATION AUTHORITY ya que no emite Certificados para Personas Físicas. Únicamente se aplicará como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY.

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 IPS CERTIFICATION AUTHORITY, 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**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA 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 la CA 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.

## **2.8. Auditorías:**

### **2.8.1 Auditorías Internas:**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

**IPS CERTIFICATION AUTHORITY, S.L. se obliga a auditar lo relacionado a su labor certificadora y sus sistemas informáticos de acuerdo a lo que, a continuación, se desarrolla.**

Los sistemas de información e instalaciones relacionadas con la labor certificadora de IPS CERTIFICATION AUTHORITY, S.L., se someterán, cada dos años, a una auditoría interna que verifique el cumplimiento del presente CPS, así como, los procedimientos e instrucciones vigentes en materia de practicas de certificación.

El Informe de dicha Auditoría determinará sobre la adecuación de las medidas y controles prevista en el presente CPS, así como identificar las deficiencias observadas y proponer las medidas correctoras o complementarias necesarias. Deberá, igualmente, incluir datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los Informes de Auditoría deben ser analizados por el una persona dentro de IPS CERTIFICATION AUTHORITY, S.L., que deberá elevar las conclusiones a la dirección de la Empresa., S.L. para que adopte las medidas correctoras adecuadas.

En concreto, las áreas que abarca la auditoria encaminadas a comprobar los mecanismos de seguridad en las actividades certificadoras desarrolladas en IPS CERTIFICATION AUTHORITY, S.L. son las siguientes:

- El desarrollo de las políticas de seguridad, es decir, los procedimientos, estándares, normas y guías de acción en relación a la labor certificadora de IPS CERTIFICATION AUTHORITY, S.L..

- Amenazas físicas externas para la CA, como son, entre otras, protecciones frente a inundaciones, incendios, explosiones, corte de líneas o de suministros u otros supuestos análogos o similares.
- Control de accesos adecuado a la información referente a la labor certificadora de IPS CERTIFICATION AUTHORITY, S.L., tanto físico como lógicos, para que cada usuario pueda acceder a los recursos a que esté autorizado, y realizar sólo las funciones permitidas.
- En materia legislativa sobre Protección de Datos de Carácter Personal, toda la legislación en cuanto a los datos de carácter personal bajo tratamiento y otros controles en cuanto a los datos e información en general, según sus características particulares.
- Topología de redes y tipo de Comunicaciones, utilización de herramientas de cifrado de la información, protección ante ataques informáticos de cualquier forma u otros supuestos análogos o similares.
- Desarrollo de aplicaciones en un entorno seguro, verificando que se incorporan controles en los productos desarrollados, y que éstos resulten auditables.
- Atención al cumplimiento de contratos y desarrollo de actividad de terceros, en tanto en cuanto estén relacionados con la labor certificadora de IPS CERTIFICATION AUTHORITY, S.L., ya sea en régimen de subcontratación parcial, outsourcing o cualquier otro tipo de contraprestación.
- Antecedentes y objetivos de la Auditoría.
- Informe ejecutivo para la dirección de la Empresa.
- Agrupación de los diferentes tipos de seguridad dentro del Informe.

El objetivo de la Auditoría básicamente consistirá en detectar posibles fallos en determinadas situaciones, entre las que se pueden mencionar, entre otras:

- La existencia de copias de respaldo de activos críticos de una manera periódica.
- El cumplimiento de la legislación aplicable, así como de las políticas y normas internas y, en especial el CPS.
- Mostrar incumplimientos, debilidades y recomendaciones. Clasificación de los puntos en diferentes niveles de importancia. Mostrar recomendaciones para solucionar los problemas encontrados.
- La responsabilidad e importancia otorgadas a las medidas de seguridad.
- Motivación de directivos y empleados en relación con la seguridad.
- Diferenciación de entornos de desarrollo y producción.
- Evaluación periódica de riesgos.

- Segregación de funciones y organización adecuada.

Las fuentes para realizar la Auditoría estarán en función de los objetivos, pero podemos destacar, entre otras las siguientes:

- Políticas, estándares, procedimientos y normas y, en especial el CPS, el que implícitamente se recoge la Norma de Certificación que IPS CERTIFICATION AUTHORITY, S.L. observa en la emisión de Certificados.
- Planes de Seguridad.
- Contratos y pólizas de seguros.
- Organigrama y descripción de funciones.
- Documentación de las aplicaciones.
- Descripción de dispositivos y algoritmos relacionados con la seguridad.
- Manuales técnicos de herramientas informáticas.
- Inventarios de soportes, aplicaciones y datos.
- Topología de Redes.
- Planos de Instalaciones.
- Entrevistas a diferentes niveles.
- Ficheros.
- Programas.
- Actas de reuniones relacionadas.
- Documentación de planes de continuidad y sus pruebas.
- Informes de suministradores y consultores.

La Auditoría se desarrollará siguiendo unas fases concretas hasta llegar a la elaboración del Informe definitivo. En concreto estas fases son las siguientes:

- Concreción de los objetivos y delimitación del alcance y profundidad de la Auditoría. Delimitación del período cubierto.
- Análisis de las posibles fuentes y recopilación de información.
- Determinación del plan de trabajo y calendario de la actividad.
- Adaptación de cuestionarios y consideración de las herramientas y perfiles de los expertos necesarios.
- Realización de entrevistas y pruebas.
- Análisis de los resultados.
- Elaboración de un informe provisional.
- Presentación y discusión del Informe provisional.
- Elaboración del Informe definitivo.

**2.8.2. Auditorías externas:**

Este apartado únicamente será de aplicación para IPS CERTIFICATION AUTHORITY. No obstante, IPS CERTIFICATION AUTHORITY se reserva el derecho de exigir a las CA's de Segundo Nivel a las que haya emitido Certificados, el sometimiento de este tipo de Auditorías.

IPS CERTIFICATION AUTHORITY se compromete a someterse al control de Auditores externos de conformidad con las normas de la AICPA. Estas auditorías se llevarán a cabo por empresas de reconocido prestigio debidamente autorizadas para llevar a cabo esta labor. El objeto de las mencionadas auditorías es determinar con imparcialidad el grado de cumplimiento de todos los Principios y Criterios WebTrust CA. Estas Auditorías se realizarán con la periodicidad que marquen las Auditores debidamente habilitados para llevar a cabo esta labor.

IPS CERTIFICATION AUTHORITY se compromete a presentar o publicar en su sitio web los sellos que demuestren que la Auditoría ha finalizado con un Informe favorable.

En relación a las auditorías señaladas, se realizarán por empresas de reconocido prestigio debidamente autorizadas para llevar a cabo esta labor, inspecciones periódicas cada tres meses determinar con el objetivo de determinar con imparcialidad si se siguen cumpliendo, por parte de IPS CERTIFICATION AUTHORITY, los Principios y Criterios WebTrust CA.

Tanto los Informes de las Auditorías, como los Informes de las inspecciones periódicas se comunicarán a la Dirección de IPS CERTIFICATION AUTHORITY con el objetivo de, si así fuera necesario, subsanar o corregir las deficiencias que se hayan podido detectar en un plazo razonable de tiempo.

### 3 IDENTIFICACIÓN Y AUTENTICACIÓN. GENERACIÓN DE CERTIFICADOS:

La identificación y autenticación del solicitante y/o el suscriptor se determinará en función de los certificados que se soliciten. Únicamente podrán ser suscriptores de Certificados de CA de Segundo Nivel personas jurídicas. En todo caso, los solicitantes y/o suscriptores de certificados deberán presentar ante la AR los siguientes documentos, con el objeto de proceder a su identificación y autenticación:

- Copia Compulsada Notarialmente de la Escritura registrada de la sociedad solicitante o suscriptora. En su defecto se deberá aportar tanto el original de la Escritura de la sociedad solicitante o suscriptora, como la copia de la misma para su cotejo por IPS CERTIFICATION AUTHORITY.
- En el caso que se actúe en nombre o representación del solicitante, Copia Compulsada Notarialmente del Poder por el que se autoriza a actuar en nombre o representación del solicitante. En su defecto se deberá aportar tanto el original del Poder por el que se autoriza a actuar en nombre o representación del solicitante, como la copia del mismo para su cotejo por IPS CERTIFICATION AUTHORITY.

#### 3.1.Certificados para CA de Segundo Nivel:

Este apartado se aplica, **ÚNICAMENTE** a IPS CERTIFICATION AUTHORITY. El término CA se refiere a IPS CERTIFICATION AUTHORITY.

La generación de certificados, incluyendo el procedimiento de identificación y autenticación, para CA de Segundo Nivel será el que a continuación se procede a detallar:

- El suscriptor y/o solicitante de este tipo de certificados deberá generar la Petición de Certificados para Firma (PCF). En todo caso esta petición deberá contener los siguientes campos:

- Common-name: El nombre de la organización solicitante y/o suscriptora. Junto con su CIF.
  - Organization Unit: Este campo será a elección del solicitante o suscriptor.
  - Localidad: Localidad donde se encuentra la organización solicitante y/o suscriptora.
  - State: Provincia donde se encuentra la organización y/o suscriptora.
  - Country: País donde se encuentra la organización solicitante y/o suscriptora.
- El procedimiento para la generación del PCF y de las claves pública y privada variará en función del tipo de servidor dedicado a emitir Certificados de la CA de Segundo Nivel. Este procedimiento de generación de claves se realiza presencialmente ante un Responsable autorizado específicamente por IPS CERTIFICATION AUTHORITY.
  - Una vez rellena el PCF, el suscriptor y/o solicitante se lo entregará al Responsable autorizado específicamente por IPS CERTIFICATION AUTHORITY señalado en el paso anterior.
  - El suscriptor y/o solicitante deberá rellenar el formulario de compra de Certificados para CA de Segundo Nivel. En todo caso dicho formulario contendrá los siguientes campos:
    - Nombre del suscriptor.
    - Domicilio: Se deberá reflejar la dirección postal, población, código postal y provincia del suscriptor.
    - CIF del suscriptor.
    - Firma del representante con Poder Bastante por el que es autorizado a actuar en nombre o representación del solicitante y/o suscriptor.
    - Persona de Contacto: Nombre de la persona que firma el formulario de compra del certificado.
    - Teléfono: Número de teléfono del suscriptor del Certificado.
    - FAX: Número de FAX del solicitante del Certificado.
    - Nombre del Servidor: Nombre del Servidor encargado de emitir Certificados de Segundo Nivel.
    - Correo Electrónico: Dirección de correo electrónico de la persona de contacto.

- Envío por Correo Postal Certificado: El solicitante y/o suscriptor deberá enviar, por correo postal certificado, o entregar en mano, los siguientes documentos a la dirección postal de la CA:
  - Copia del PCF, que contendrá la Clave Pública, generado por el servidor que se encargará de emitir Certificados de la CA de Segundo Nivel.
  - Formulario de compra de Certificados para CA de Segundo Nivel con todos sus campos rellenos correctamente.
  - Copia del justificante de la transferencia bancaria o talón a nombre de IPS CERTIFICATION AUTHORITY, dependiendo del método de pago elegido. La cantidad de la transferencia bancaria o del talón dependerá del acuerdo particular al que hayan llegado el suscriptor e IPS CERTIFICATION AUTHORITY. Dicho acuerdo estará reflejado en un Contrato de licencia para certificación digital para CA de Segundo Nivel.
  - Copia Compulsada Notarialmente de la Escritura de Constitución del suscriptor debidamente registrada. En su defecto se deberá aportar tanto el original de la Escritura de la sociedad solicitante o suscriptora, como la copia de la misma para su cotejo por IPS CERTIFICATION AUTHORITY.
  - Copia Compulsada Notarialmente del Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor. En su defecto se deberá aportar tanto el original del Poder por el que se autoriza a actuar en nombre o representación del solicitante, como la copia del mismo para su cotejo por IPS CERTIFICATION AUTHORITY.
  -
- La CA procederá a la comprobación que los datos reflejados en la Escritura de Constitución del suscriptor debidamente registrada y en el Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor, se corresponden con los datos reflejados en la solicitud de PCF enviada por el solicitante y/o suscriptor.
- La CA procederá a la emisión del Certificado para CA de Segundo Nivel una vez firmado el contrato de CA de Segundo Nivel por el representante del solicitante y/o suscriptor y comprobada la transferencia bancaria, o una vez ingresado el talón a nombre de IPS CERTIFICATION AUTHORITY en su cuenta corriente. La firma del

contrato de CA de Segundo Nivel podrá realizarse ante fedatario público, a discreción de IPS CERTIFICATION AUTHORITY o del solicitante y/o suscriptor. Inmediatamente después de la emisión del Certificado IPS CERTIFICATION AUTHORITY comunicará al suscriptor/solicitante el hecho de dicha emisión a través de correo electrónico.

- Una vez emitido el Certificado por la CA, ésta comprobará el contenido del Certificado en busca de errores u omisiones y será entregado en mano al solicitante/suscriptor por personal autorizado de IPS CERTIFICATION AUTHORITY.

La extensión de los campos de los Certificados de IPS CERTIFICATION AUTHORITY se encuentra recogida en el apartado 10.1 del presente CPS.

Con respecto a la re-emisión de certificados, las peticiones recibirán el mismo tratamiento y se realizarán las mismas comprobaciones que si de un certificado nuevo se tratase.

### **3.2. Certificados que podrán emitir las CA de Segundo Nivel:**

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

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

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

La generación de certificados B1, incluyendo el procedimiento de identificación y autenticación, deberá coincidir con el que a continuación se procede a detallar:

- El solicitante y/o suscriptor deberá comunicar a la AR, a través de medios telemáticos (por ejemplo, a través de un formulario en la página

web de la AR) la dirección de correo electrónico a la que va dirigido el Certificado B1. Asimismo, el solicitante y/o suscriptor deberá introducir, igualmente por medios telemáticos, un password o contraseña.

- El solicitante recibirá de la AR una notificación, en la dirección de correo electrónico que ha indicado, para poder realizar la petición del Certificado B1. El solicitante y/o suscriptor deberá acceder a la petición de Certificado B1 a través de medios telemáticos (por ejemplo, la Notificación para poder realizar la petición del Certificado B1 podrá consistir en un correo electrónico que incluya un enlace a la página web de la AR).
- La AR comprobará, a través de medios telemáticos, que la dirección de correo electrónico concuerda efectivamente con la dirección de correo electrónico al que va dirigido el Certificado B1 (por ejemplo, la AR comprobará la dirección de correo solicitando el password o contraseña introducido por el solicitante y/o suscriptor al inicio del procedimiento).
- El solicitante y/o suscriptor procederá al envío, a través de medios telemáticos, de la petición de Certificado B1 (por ejemplo, a través de un formulario en la página web de la AR) junto con los datos suficientes (por ejemplo número de tarjeta de crédito) para poder procederle al cobro.
- La AR comunicará a la CA, que los datos recogidos en la solicitud de Certificado B1 del solicitante y/o suscriptor coinciden con los datos aportados por el solicitante y/o suscriptor.
- La CA generará en el equipo del suscriptor y/o solicitante las clave pública y clave privada.
- La CA procederá al envío al solicitante y/o suscriptor del Certificado B1.

### **3.2.2. B2. Certificado Personal con verificación documental**

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

La generación de certificados B2, incluyendo el procedimiento de identificación y autenticación, deberá coincidir con el que a continuación se procede a detallar:

- El solicitante y/o suscriptor deberá a comunicar a la AR los siguientes datos:
  - Nombre: Se deberá recoger el nombre del suscriptor.
  - E-mail: El suscriptor y/o solicitante deberá aportar su dirección de correo electrónico a la AR.
  - Ciudad: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Localidad donde reside.
  - Estado: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Provincia donde reside.
  - País: El suscriptor y/o solicitante deberá aportar a la AR el nombre del País donde reside.
  - Otros datos: Cualquier otro dato que pueda resultar de interés para el solicitante y/o suscriptor, para la CA o para la AR.
- La comunicación de los datos reflejados en el punto anterior podrá realizarse a través de Internet, o a través de correo postal.
- El solicitante y/o suscriptor deberá enviar a la AR a través de correo postal o FAX una copia de su Documento Nacional de Identidad.
- La AR comprobará la veracidad de los datos enviados por el solicitante y/o suscriptor. Para ello, procederá a la verificación de que los datos reflejados en la copia del Documento Nacional de Identidad del solicitante y/o suscriptor, coinciden con los datos recogidos en la solicitud de Certificado B2 remitida por el solicitante y/o suscriptor.
- La AR comunicará a la CA, que los datos recogidos en la solicitud de Certificado B2 del solicitante y/o suscriptor coinciden con los datos recogidos en la copia de Documento Nacional de Identidad remitida por el solicitante y/o suscriptor.
- El solicitante y/o suscriptor procederá a realizar una transferencia bancaria a favor de la CA o a emitir un talón a favor de la CA por la cantidad que la mencionada CA estipule.
- La CA procederá a la emisión del Certificado B2 una vez comprobada la transferencia bancaria, o una vez ingresado el talón a nombre de la CA en su cuenta corriente.

### **3.2.3. B3. Certificado Personal Presencial:**

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

La generación de certificados B3, incluyendo el procedimiento de identificación y autenticación, deberá coincidir con el que a continuación se procede a detallar:

- El solicitante y/o suscriptor deberá a comunicar a la AR los siguientes datos:
  - Nombre: Se deberá recoger el nombre del suscriptor.
  - E-mail: El suscriptor y/o solicitante deberá aportar su dirección de correo electrónico a la AR.
  - Ciudad: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Localidad donde reside.
  - Estado: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Provincia donde reside.
  - País: El suscriptor y/o solicitante deberá aportar a la AR el nombre del País donde reside.
  - Otros datos: Cualquier otro dato que pueda resultar de interés para el solicitante y/o suscriptor , para la CA o para la AR.
  
- La comunicación de los datos reflejados en el punto anterior podrá realizarse a través de Internet, o a través de correo postal.
- El solicitante y/o suscriptor deberá personarse ante la AR portando su Documento Nacional de Identidad.
- La AR comprobará la veracidad de los datos enviados por el solicitante y/o suscriptor. Para ello, procederá a la verificación de que los datos reflejados Documento Nacional de Identidad del solicitante y/o suscriptor, coinciden con los datos recogidos en la solicitud de Certificado B3 remitida por el solicitante y/o suscriptor.
- La AR y el solicitante y/o suscriptor suscribirán un documento privado en el que se recoja que los datos aportados por el solicitante y/o suscriptor y los reflejados en su Documento Nacional de Identidad son los mismos. Además en ese documento la AR declarará que la persona ante ella personada corresponde en suficiente apariencia, con la imagen contenida en el Documento Nacional de Identidad por dicha persona aportada.

- La AR remitirá a la CA copia del documento privado suscrito entre el solicitante y/o suscriptor y la propia AR
- El solicitante y/o suscriptor procederá a realizar una transferencia bancaria a favor de la CA o a emitir un talón a favor de la CA por la cantidad que la mencionada CA estipule.
- La CA procederá a la emisión del Certificado B3 una vez comprobada la transferencia bancaria, o una vez ingresado el talón a nombre de la CA en su cuenta corriente.

#### **3.2.4. B4. Certificado Personal Presencial ante Fedatario Público:**

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

La generación de certificados B4, incluyendo el procedimiento de identificación y autenticación, deberá coincidir con el que a continuación se procede a detallar:

- El solicitante y/o suscriptor deberá a comunicar a la AR los siguientes datos:
  - Nombre: Se deberá recoger el nombre del suscriptor.
  - E-mail: El suscriptor y/o solicitante deberá aportar su dirección de correo electrónico a la AR.
  - Ciudad: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Localidad donde reside.
  - Estado: El suscriptor y/o solicitante deberá aportar a la AR el nombre de la Provincia donde reside.
  - País: El suscriptor y/o solicitante deberá aportar a la AR el nombre del País donde reside.
  - Otros datos: Cualquier otro dato que pueda resultar de interés para el solicitante y/o suscriptor , para la CA o para la AR.
- La comunicación de los datos reflejados en el punto anterior podrá realizarse a través de Internet, o a través de correo postal.
- El solicitante y/o suscriptor deberá personarse ante la AR portando su Documento Nacional de Identidad y Documento Público emitido por un

Notario en el que conste que la persona ante él personada corresponde en suficiente apariencia, con la imagen contenida en el Documento Nacional de Identidad por dicha persona aportado.

- La AR comprobará la veracidad de los datos enviados por el solicitante y/o suscriptor. Para ello, procederá a la verificación de que los datos reflejados Documento Nacional de Identidad del solicitante y/o suscriptor y en Documento Público emitido por el Notario, coinciden con los datos recogidos en la solicitud de Certificado B4 remitida por el solicitante y/o suscriptor.
- La AR remitirá a la CA copia del Documento Público emitido por el Notario en el que conste que la persona ante él personada corresponde en suficiente apariencia, con la imagen contenida en el Documento Nacional de Identidad por dicha persona aportado.
- El solicitante y/o suscriptor procederá a realizar una transferencia bancaria a favor de la CA o a emitir un talón a favor de la CA por la cantidad que la mencionada CA estipule.
- La CA procederá a la emisión del Certificado B4 una vez comprobada la transferencia bancaria, o una vez ingresado el talón a nombre de la CA en su cuenta corriente.

### **3.2.5. A1. Certificados de Servidor:**

Este apartado se aplica **ÚNICAMENTE** a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá para referirse a una CA de Segundo Nivel.

La emisión de un certificado de servidor implica el reconocimiento de la identidad de la empresa solicitante, tener registrado el dominio de Internet bajo el que se denomina el servidor y cumplir con el procedimiento que a continuación se detalla:

- El suscriptor y/o solicitante de este tipo de certificados deberá generar la Petición de Certificados para Firma (PCF). En todo caso esta petición deberá contener los siguientes campos:
  - Common-name: El nombre en Internet de la organización o persona solicitante y/o suscriptora.

- Organization Unit: Este campo será a elección del solicitante o suscriptor.
  - Localidad: Localidad donde se encuentra la organización o persona solicitante y/o suscriptora.
  - State: Provincia donde se encuentra la organización o persona solicitante y/o suscriptora.
  - Country: País donde se encuentra la organización o persona solicitante y/o suscriptora.
- El procedimiento para la generación del PCF y de las claves pública y privada variará en función del tipo de servidor en el que se instale el Certificado de Servidor.
  - Una vez rellena el PCF, el suscriptor y/o solicitante deberá enviarla, junto la clave pública que se ha generado, a una dirección de correo electrónico de la AR.
  - El suscriptor y/o solicitante deberá rellenar el formulario de compra de Certificados de Servidor. En todo caso dicho formulario contendrá los siguientes campos:
    - Nombre del suscriptor.
    - Domicilio: Se deberá reflejar la dirección postal, población, código postal y provincia del suscriptor.
    - NIF/CIF del suscriptor.
    - Firma del solicitante y/o suscriptor o, en su caso, firma de su representante con Poder Bastante por el que es autorizado a actuar en nombre o representación del solicitante y/o suscriptor.
    - Persona de Contacto: Nombre de la persona que firma el formulario de compra del certificado.
    - Teléfono: Número de teléfono del suscriptor del Certificado.
    - FAX: Número de FAX del solicitante del Certificado.
    - Nombre del Servidor: Nombre del Servidor donde se va a instalar el Certificado de Servidor.
    - Correo Electrónico: Dirección de correo electrónico de la persona de contacto.
  - Envío por Correo Postal Certificado: El solicitante y/o suscriptor deberá enviar, por correo postal certificado, los siguientes documentos a la dirección postal de la AR:
    - Copia del PCF, que contendrá la Clave Pública, generado por el servidor donde se instalará el Certificado de Servidor.

- Formulario de compra de Certificados para Certificado de Servidor con todos sus campos rellenos correctamente.
  - Copia del justificante de la transferencia bancaria o talón a nombre de la CA, dependiendo del método de pago elegido.
  - Copia de la Escritura de Constitución del suscriptor debidamente registrada. No obstante la AR y la CA se reservarán el derecho a solicitar, antes de la emisión de certificados de servidor o después de la mencionada emisión, Copia Compulsada de la Escritura de Constitución del suscriptor.
  - Copia del Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor. No obstante la AR y la CA se reservarán el derecho a solicitar, antes de la emisión de certificados de Servidor o después de la mencionada emisión, Copia Compulsada del Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor.
- La AR procederá a la comprobación que los datos reflejados en la Escritura de Constitución del suscriptor debidamente registrada y en el Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor se corresponden con los datos reflejados en la solicitud de PCF enviada por el solicitante y/o suscriptor.
  - La AR comunicará a la CA, que los datos recogidos en la solicitud de Certificado de Servidor del solicitante y/o suscriptor coinciden con los datos recogidos en la Copia de la Escritura de Constitución del Solicitante y, en su caso, Copia del Poder por el que se autoriza a actuar en nombre o representación del solicitante y/o suscriptor.
  - La CA procederá a la emisión del Certificado de Servidor una vez comprobada la transferencia bancaria, o una vez ingresado el talón a nombre de la CA en su cuenta corriente.

## **4 GESTIÓN DE LAS CLAVES:**

### **4.1. Aspectos Generales:**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La clave privada de la CA tendrá como **ÚNICAS** utilidades la firma de la clave pública del suscriptor/solicitante, en definitiva, la emisión de un Certificado a favor del suscriptor/solicitante y la firma de las CRL. La clave pública de la CA tendrá como objetivo verificar la firma de la CA. En general, la CA seguirá una serie de estándares o normas a la hora de generar el par de claves, tanto los de la CA, como los del suscriptor/solicitante. Estas normas o estándares son los siguientes:

- El tamaño de las claves será como mínimo de 2048 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- El estándar para el módulo criptográfico de generación de claves es el FIPS CERTIFICATION AUTHORITY 140-1 level 3, en caso de utilizar hardware.
- El período de validez de las claves va a ser, como máximo, de diez años, o el máximo establecido por la legislación vigente.

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

Este apartado se aplica **ÚNICAMENTE** a IPS CERTIFICATION AUTHORITY. El término CA se entenderá para referirse a IPS CERTIFICATION AUTHORITY.

El procedimiento de generación de las claves es el siguiente

Las claves de la CA IPS CERTIFICATION AUTHORITY SERVIDORES, certificado raíz de IPS CERTIFICATION AUTHORITY, se generaron mediante software, sobre un sistema informático seguro, con las medidas que la tecnología proporcionaba en el año 1998.

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 IPS CERTIFICATION AUTHORITY.

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 sobreescritura.

### **4.3. Gestión de las claves del solicitante/suscriptor:**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

El procedimiento para la generación de las claves es el siguiente:

Los suscriptores generan sus claves fuera de las instalaciones de la CA, bajo su responsabilidad, sin el control directo de la CA. Esta generación la pueden realizar mediante dispositivos hardware o software. La CA sólo generará claves sobre dispositivos criptográficos y en ningún caso almacenará copias de estas claves, salvo acuerdo específico con el cliente y a efectos de copia de seguridad para operaciones de cifrado, nunca se almacenarán claves de firma.

La CA no proporciona ningún tipo de servicio de gestión de las claves al solicitante/suscriptor.

La distribución de la clave pública del suscriptor/solicitante por parte de la CA será a través del envío de dicha clave al suscriptor/solicitante mediante mecanismos de web o correo electrónico. No obstante, en determinadas ocasiones y siempre que la CA y el suscriptor/solicitante lo acuerden, la distribución de la clave pública será a través del acceso a un repositorio de claves públicas. El mencionado acceso se realizará a través de la página web de la CA .

Si fuera necesario proceder al cambio de claves del suscriptor, éste cambio sólo será posible con la generación de un nuevo par de claves.

El procedimiento para proporcionar una nueva clave pública al solicitante/suscriptor será a través del envío, por parte de la CA de un PKCS#10.

El proceso para proteger las claves del suscriptor dependerá del mecanismo técnico de generación y almacenamiento adoptado por este.

## **5 REVOCACIÓN Y SUSPENSIÓN DE CERTIFICADOS**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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.

### **5.1 Supuestos de revocación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Los Certificados deberán ser revocados cuando concurra 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 sobrevinida, 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.
- En el caso de los Certificados de Apoderados de Empresa, además será causa de revocación la extinción de la Persona Jurídica representada.
- En el caso de los Certificados de Empresa sin Poderes, también será causa de revocación la propia revocación de la autorización al suscriptor para la utilización del certificado en virtud del cual se identifica en el mercado como persona relacionada con dicha entidad.

#### **5.1.1 Efectos de la revocación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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. Las causas que motivan una revocación es una información no considerada confidencial por IPS CERTIFICATION AUTHORITY, por tal motivo IPS CERTIFICATION AUTHORITY se reserva el derecho de publicarla en la CRL.

## **5.2 Supuestos de suspensión**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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.

### **5.2.1 Efectos y límites de la Suspensión**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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.

### **5.3 Procedimiento de suspensión y revocación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

#### **5.3.1 Legitimación activa**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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, IPS CERTIFICATION AUTHORITY 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 el Real Decreto Ley de Firma Electrónica 14/1999, de 17 de septiembre, así como las demás disposiciones vigentes, instar a la CA a suspender/revocar el certificado.

### **5.3.2 Recepción de solicitudes de suspensión/revocación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La solicitud de suspensión/revocación de Certificados se podrá dirigir a la CA en la forma de comunicación telefónica a través del siguiente número: +34 91 630.85 68

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 IPS CERTIFICATION AUTHORITY a efectos probatorios.

En caso de petición de revocación por parte del suscriptor, un representante de él deberá enviar a la dirección postal de la CA, a fin de poder ejercitar su derecho de suspensión/revocación los siguientes documentos:

- Copia del DNI del representante autorizado.
- Documento explicativo en el que conste las razones o motivos para la petición de revocación del Certificado.
- Copia Compulsada Notarialmente de un Poder en el que conste su facultad para instar la revocación.

- Copia Compulsada Notarialmente de la escritura de constitución del solicitante/suscriptor.
- Copia Compulsada Notarialmente del CIF del solicitante/suscriptor.

Comprobados los datos aportados por el representante del solicitante/suscriptor, IPS CERTIFICATION AUTHORITY procederá a verificar por el medio que considere oportuno, la intención de revocar por parte del solicitante/suscriptor y procederá a la revocación del Certificado.

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.

### **5.3.3 Decisión de suspender/revocar**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

IPS CERTIFICATION AUTHORITY no concede ningún período de gracia a favor del solicitante/suscriptor de un Certificado en una solicitud de revocación de su Certificado.

### **5.3.4 Comunicación y Publicación de la suspensión/revocación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La decisión de suspender/revocar el Certificado será comunicada por la CA al Suscriptor mediante correo ordinario.

Igualmente, se publicará la suspensión/revocación del Certificado en la CRL.

La suspensión/revocación comenzará a producir efectos a partir de su publicación por parte de la CA, salvo que la causa de revocación sea el cese de la actividad de la CA, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

## **6 CADUCIDAD DE CERTIFICADOS**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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.

## **7 RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN**

### **7.1 Renovación de Certificados**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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 un nuevo Certificado 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 IPS CERTIFICATION AUTHORITY 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 de IPS CERTIFICATION AUTHORITY si concurren los extremos generales que a continuación se detallan.

#### **7.1.1 Requisitos previos**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Deberán concurrir los siguientes:

- IPS CERTIFICATION AUTHORITY comunicará a los suscriptores, 45 días antes de la caducidad de sus Certificados, la necesidad de la renovación del mismo. Esta comunicación será realizada por correo electrónico.
- 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 IPS CERTIFICATION AUTHORITY 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.

### **7.1.2 Cómo solicitar la renovación**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

El suscriptor que solicite la renovación de los servicios de certificación deberá cumplimentar un formulario que la CA pondrá a su disposición en formato papel.

El suscriptor enviará ese formulario debidamente cumplimentado a la AR 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.

La AR procederá a la verificación y validación de la identidad del suscriptor que ha solicitado la renovación de su Certificado. Una verificada y validada la identidad, la AR remitirá el formulario a la CA.

Además del envío de la solicitud, el suscriptor deberá abonar 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, no le serán devueltas y no tendrá derecho a reclamarlas a IPS CERTIFICATION AUTHORITY.

### **7.1.3 Procedimiento de renovación de certificados**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Cuando la CA reciba la solicitud del suscriptor en debida forma, procederá a la generación de nuevas claves criptográficas y emitirá un nuevo 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 ese Certificado 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.

## 7.2 Reemisión de certificados

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Este procedimiento se establece para los casos en que el Certificado de un Suscriptor sea declarado revocado por la existencia de inexactitudes en el Certificado o éste se haya dejado caducar sin que se haya llegado a instar la renovación con anterioridad a los treinta últimos días su vigencia.

En los casos señalados en el párrafo anterior el suscriptor/solicitante deberá seguir los procedimientos establecidos para la solicitud de un Certificado nuevo. (Apartado 3.3 del CPS)

## 7.3. Regeneración de claves:

Este apartado se aplica, **ÚNICAMENTE** a IPS CERTIFICATION AUTHORITY.

IPS CERTIFICATION AUTHORITY no gestiona ningún tipo de procedimiento de regeneración de las claves del suscriptor/solicitante. Lo que únicamente IPS CERTIFICATION AUTHORITY gestiona es la revocación o la reemisión de Certificados según lo establecido en los apartados precedentes.

## 8 EXTINCIÓN DE LA CA

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

En orden a causar el menor daño posible tanto a los Suscriptores como a los Usuarios del sistema de certificación ante un hipotético cese de la CA y de acuerdo con el artículo 21 de la ley 59/2003 de Firma Electrónica, IPS Certification AuthorityCA realizará todas las gestiones necesarias para transferir, con el consentimiento expreso de los suscriptores, la gestión de los certificados que sigan en vigor en la fecha en que se produzca el cese, a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir la vigencia. Para la consecución de estos objetivos se establecen las siguientes medidas:

- . • Establecer, cuando ello fuera posible, un acuerdo con otro Prestador del Servicio de Certificación con el propósito de transmitir todas sus obligaciones y derechos dentro del sistema de certificación con la intención de continuar el servicio. Si se produce la subrogación, esta CPS seguirá siendo el documento que establece las relaciones entre las partes mientras no se establezca un nuevo documento por escrito.
- . • Comunicará fehacientemente, y con una antelación mínima de dos meses el cese de la actividad, informando al mismo tiempo sobre todas las características del Prestador de Servicios de Certificación al que se propone la transferencia de la gestión de los certificados.
- . • Recabar el consentimiento expreso de los suscriptores que tengan en ese momento certificados que estén en vigor para la transferencia de la gestión de

los certificados.

- . • 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.
- . • Informar a las administraciones competentes, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando en su caso si se va a transferir la gestión y a quien.
- . • Con carácter previo al cese definitivo de la actividad, comunicará a la administración competente la información relativa a los certificados expedidos al público cuya vigencia haya sido extinguida para que se haga cargo de su custodia a los efectos del artículo 20.1 f) DE LA LEY 5972003
- . • Cualquier otra obligación que venga impuesta por la ley.

## **9 CONTROLES DE SEGURIDAD**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

### **9.1 Manual Interno de Seguridad**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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 IPS CERTIFICATION AUTHORITY. 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 IPS CERTIFICATION AUTHORITY. 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.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA 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.

La CA 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.

### **9.3. Seguridad del Personal.**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Los empleados de la CA que acceden o tratan información de la empresa generadora de negocio y, en especial, información relacionada con la labor certificadora de IPS CERTIFICATION AUTHORITY firman un acuerdo de confidencialidad con la CA.

Los empleados de la CA reciben instrucciones por escrito instándoles a la utilización de los recursos de IPS CERTIFICATION AUTHORITY y, en especial, de los recursos relacionados con la labor certificadora de la CA con la única intención de ser usados para los propósitos del negocio.

Todos los empleados de la CA reciben documentación de seguridad de las tecnologías de la información y, en especial, de seguridad en la labor certificadora de IPS CERTIFICATION AUTHORITY. Además, reciben el correspondiente adiestramiento para acometer dicha labor.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Los servidores y sistemas multiusuarios que dan soporte a las actividades del negocio de la CA y, en especial, a la labor certificadora, están ubicados en zonas seguras para su uso exclusivo dedicado a tal fin. Además, el acceso a los mencionados servidores y sistemas multiusuarios está restringido y sólo se permite la entrada a personal debidamente autorizado.

El cableado utilizado para las comunicaciones internas o externas termina en áreas segura de uso exclusivo y el acceso a las mismas está restringido y sólo se permite la entrada a personal debidamente autorizado.

El equipo para el proceso de la información que alberga la CA de IPS CERTIFICATION AUTHORITY se encuentra offline en un lugar fuera de las instalaciones de IPS CERTIFICATION AUTHORITY con las siguientes medidas de seguridad:

- Control de acceso físico al lugar donde se encuentra la CA.
- Dispositivo que permite el bloqueo del lugar donde se encuentra la CA.
- Sistemas de apertura automática.
- Detectores sísmicos, microfónicos u otros dispositivos que permitan detectar cualquier ataque a través de techos, paredes o suelos de las cámaras acorazadas o de las cajas de alquiler.
- Detectores volumétricos.
- Mirillas ojo de pez o dispositivos similares, o circuito cerrado de televisión en su interior, conectado con la detección volumétrica o provistos de videosensor, con proyección de imágenes en un monitor visible desde el exterior.
- Sistemas de aire acondicionado.
- Sistema contra inundaciones.
- Sistema de prevención de incendios.

IPS CERTIFICATION AUTHORITY cumple con las normas establecidas en el edificio donde se encuentran sus oficinas en cuanto a la recogida y tratamiento de residuos.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el

término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA cuenta con procedimientos, regulados de forma escrita, regulados para la operación de todos los sistemas de ordenador. Además los sistemas que están soportando aplicaciones de negocios y, en especial, los relacionados con la labor certificadora, son mantenidos conforme a listas de comprobación específicas o métodos similares mediante los que se garantice un nivel apropiado de seguridad en cada uno de ellos.

La CA dispone de un registro de administración para cada sistema crítico y en especial, los relacionados con la labor certificadora de IPS CERTIFICATION AUTHORITY, con el fin de que el negocio que se revise, al menos, semanalmente.

La CA dispone de medidas para la detección y prevención de virus en todos los ordenadores personales de los usuarios y en los servidores. Estas herramientas se actualizan regularmente.

La CA cuenta con instrucciones escritas dirigidas a sus empleados con el fin de establecer un procedimiento encaminado a notificar cualquier tipo de incidente relacionado con virus y que acciones tomar o no tomar en caso que se produzcan algún incidente y, en especial, una infección.

Cada sistema multiusuario cuenta con procedimientos adecuados documentados para su recuperación en caso de fallo. Estos procedimientos son de aplicación asimismo para sistemas monousuario que contengan información crítica o sensible para el negocio y, en especial, aquella información relacionada con la labor certificadora de IPS CERTIFICATION AUTHORITY.

Los procedimientos de recuperación en caso de fallo señalados en el párrafo anterior son revisados y comprobados una vez cada seis meses.

IPS CERTIFICATION AUTHORITY realiza semanalmente copias de seguridad de los datos que posee y, en especial, los relacionados con su labor certificadora.

Los soportes en los que se contienen las copias de seguridad de la información de IPS CERTIFICATION AUTHORITY y, en especial, la información relativa a su labor

certificadora, están ubicados en un lugar, ubicado a menos de 600 kilómetros de las oficinas de IPS CERTIFICATION AUTHORITY, tal que, en caso de desastre como, por ejemplo, incendio o inundaciones, en la oficina principal de IPS CERTIFICATION AUTHORITY, escaparían de los daños que pudieran sufrir.

La CA dispone de un procedimiento, que se encuentra recogido en formato escrito, en el que se detalla el registro de usuarios y la gestión de permisos. Concretamente este procedimiento describe como se realizan las siguientes actuaciones:

- Gestión del control de acceso.
- Creación de usuarios.
- Eliminación de usuarios.
- Cambio de los permisos de accesos.
- Eliminación inmediata de los permisos de acceso cuando ya no se necesiten.

La CA dispone de un procedimiento, que se encuentra recogido de forma escrita, en el que especifica la forma en que se comunican las contraseñas a los usuarios de los sistemas de IPS CERTIFICATION AUTHORITY, es decir, a sus empleados.

IPS CERTIFICATION AUTHORITY revisa trimestralmente la gestión de los identificadores y de los permisos de acceso a sus sistemas. Igualmente, cada tres meses, se procede a la eliminación de los identificadores de usuario inactivos.

El acceso a los sistemas de información de la CA se realizará a través de un procedimiento seguro de inicio de sesión. En este sistema se cuenta con un técnica de contraseñas efectivo que se utiliza para autenticar a los usuarios. El sistema de contraseñas se ajusta a una serie de directrices marcadas por la CA.

Los ordenadores y terminales de la CA y, en especial, los que se dediquen a la labor certificadora de IPS CERTIFICATION AUTHORITY, que se queden inactivos durante periodos de tiempo prolongados contienen un mecanismo de desconexión automática para evitar que sean utilizados por personas no autorizadas. Como mínimo cuentan con un protector de pantalla protegido por contraseña.

El acceso a los datos y los sistemas de la CA y, en especial los que se dediquen a la labor certificadora de IPS CERTIFICATION AUTHORITY, se rigen por una serie de directrices. En concreto, estas directrices son:

- No se permite el acceso de escritura a los archivos del sistema.
- Los permisos de acceso a un archivo creado por un usuario, por defecto protegen al archivo contra el acceso por parte de otros usuarios.
- Los archivos están protegidos contra acceso o modificación por parte de usuarios del mismo grupo como norma general.
- Los directorios públicos son identificados y monitorizados durante la vida del sistema para asegurar que la cantidad de tales directorios solamente cambia de acuerdo a las especificaciones del Gerente de Seguridad.
- Si se ponen a disposición pública directorios para la distribución de información no se habilita el permiso general de escritura. Para proteger la integridad de la información solamente se cuenta con permiso de lectura.

La CA ha habilitado diferentes funciones de seguimiento del uso del sistema (auditoría). Los registros son revisados al menos semanalmente y son conservados durante dos años al menos.

La CA posee una política ante la instalación de nuevas versiones o parches del sistema y, en especial los dedicados a la labor certificadora de IPS CERTIFICATION AUTHORITY. Así, se efectúa una copia de seguridad antes y después de la instalación.

## **9.6. Seguridad para usuarios de sistemas**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA cuenta con un procedimiento escrito sobre cómo deberán notificar los usuarios los incidentes de seguridad y mal funcionamiento del software. Este procedimiento está puesto a disposición de los usuarios.

Los usuarios, es decir, los empleados de IPS CERTIFICATION AUTHORITY han recibido formación e instrucciones escritas en atención a las siguientes cuestiones:

- El uso de las contraseñas.
- Las copias de seguridad de datos y software críticos, es especial los relacionados con la labor certificadora de IPS CERTIFICATION AUTHORITY.
- El uso de programas y otras aplicaciones antivirus.
- Las medidas a tener en cuenta cuando se abandona momentáneamente el equipo de trabajo
- El manejo de equipos que estén fuera de las premisas de seguridad, como es el caso, por ejemplo de los portátiles.
- La protección de la información en el correo electrónico.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA cuenta con un plan de continuidad del negocio para proteger sistemas críticos y, en especial los relacionados con la labor certificadora de IPS CERTIFICATION AUTHORITY, de fallos o desastres. El mencionado plan establece un tiempo razonable de restauración, no superior a 24 horas, de las operaciones y de los sistemas informáticos, en especial, los relacionados con la labor certificadora de IPS CERTIFICATION AUTHORITY, tras una interrupción, por cualquier motivo, de esta labor. El mencionado plan es comprobado regularmente y actualizado.

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

### **9.8 Incidencias**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Incidencia es cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos o al acceso de las distintas plataformas informáticas. En concreto, se entenderá por incidencia:

- Modificaciones no autorizadas de información.
- Acceso o intento de accesos a ficheros no autorizadas para ello.
- Copias o intento de copias indebidas de datos en los puestos de trabajo.
- Mal funcionamiento durante la realización de copias de seguridad y/o respaldo.
- Errores en el sistema informático, en las transacciones de información o en las Bases de Datos.
- Accesos no autorizados a lugares donde se ubican los sistemas y soportes informáticos.
- Cualquier otra anomalía que afecte o pudiera afectar a la seguridad de los datos o al acceso de las distintas plataformas informáticas.

IPS CERTIFICATION AUTHORITY 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 quedaran almacenadas en un registro de incidencias, en el que se guardarán datos de los dos últimos años. Mensualmente el registro de incidencias es revisado por un Responsable de IPS CERTIFICATION AUTHORITY.

### **9.9. Cumplimiento.**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Todo el software utilizado en la CA y, en especial el referido a la labor certificadora de IPS CERTIFICATION AUTHORITY es usado de conformidad con los requisitos

establecidos en la legislación vigente y, en su caso, con los requisitos establecidos en las relaciones contractuales que la CA pudiera tener.

La CA cuenta con un procedimiento, recogido en formato escrito, sobre como se salvaguardan los registros de IPS CERTIFICATION AUTHORITY, y en especial los relacionados a la labor certificadora de la CA, de pérdidas, destrucción y falsificación.

Todos los empleados que proceden al tratamiento de datos de carácter 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, IPS CERTIFICATION AUTHORITY ha elaborado e implementado un Documento de Seguridad.

## **10 CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS**

### **10.1 Características del Certificado**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Dependiendo del tipo de certificado, este podrá ser emitido en soporte de archivo de software o sobre dispositivos criptográficos.

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

El contenido de los Certificados de IPS CERTIFICATION AUTHORITY es el siguiente:

- Número de Versión.
- Número de Serie.
- Algoritmo de firma.
- Emisor.
- Fecha y hora de emisión.
- Fecha y hora de caducidad.
- Asunto.
- Clave pública.
- Extensiones.
- Algoritmo de identificación.
- Huella digital.
- Uso de la clave.

En cualquier caso, y dado el amplio ámbito de emisión, el contenido de los certificados que se emitan se determinará de manera contractual.

Con respecto a la re-emisión de certificados, las peticiones recibirán el mismo tratamiento y se realizarán las mismas comprobaciones que si de un certificado nuevo se tratase.

El formato de los Certificados emitidos por IPS CERTIFICATION AUTHORITY es PKCS#10

## **10.2 Listas de Certificados**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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 CA.

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

El Listado de Certificados en Vigor estará a disposición de los usuarios en el servidor web de la CA

El Listado de Certificados suspendidos o revocados (CRL) estará a disposición de los usuarios en el servidor web de la CA

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.

La CRL se publica una vez al mes en el servidor web de la CA. En el caso de revocación de Certificados, la CRL se publicará inmediatamente después de esta

revocación.

Los Usuarios de Certificados pueden consultar en cualquier momento el estado de un Certificado determinado, bien visitando el servidor web, bien realizando la solicitud correspondiente a través del siguiente número de teléfono: +34 91 630.85.68

El contenido de las CRL's publicadas por IPS CERTIFICATION AUTHORITY es el siguiente:

- Número de Versión.
- Algoritmo de firma.
- Emisor.
- Fecha y hora de emisión.
- Fecha y hora de la próxima publicación.
- Extensiones.

### **10.3 Consulta de estado de Certificados o revocación on line:**

Actualmente no existe disponibilidad de Consultar el estado de un Certificado o la revocación de certificados de forma on-line

## **11 OTRAS CUESTIONES.**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

La CA podrá modificar las estipulaciones de la presente CPS y de sus PRÁCTICAS DE CERTIFICACIÓN, incluidas implícitamente en su CPS, 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.

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

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

Las modificaciones efectuadas sobre la CPS o las Prácticas de Certificación, incluidas implícitamente en su CPS, de acuerdo a lo establecido en el apartado 11.4 de la presente CPS, se darán a conocer a los interesados en la página web de CA [www.ips.es](http://www.ips.es) y en las oficinas de la CA y las AR.

### **11.3 Procedimiento de notificación de las publicaciones**

Este apartado se aplica, tanto a IPS CERTIFICATION AUTHORITY, como a las CA's de Segundo Nivel que posean Certificados de IPS CERTIFICATION AUTHORITY y el término CA se entenderá tanto para referirse a IPS CERTIFICATION AUTHORITY, como para referirse a una CA de Segundo Nivel.

En caso que las modificaciones efectuadas en la CPS o en las Prácticas de Certificación, incluidas implícitamente en su CPS, 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, incluidas implícitamente en su CPS, 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.

### **11.4. Procedimiento de aprobación del CPS:**

Cuando fuera necesario realizar una modificación en la CPS, en el que están incluidas implícitamente las Prácticas de Certificación, se procederá de la siguiente forma:

- Se procederá a la modificación de los apartados específicos en el CPS original, en el que están incluidas implícitamente las Prácticas de Certificación, original.
- Se verificará las posibles relaciones de los textos modificados, en relación con la CPS completo, en el que están incluidas implícitamente las Prácticas de Certificación.

- Se procederá a comprobar la nueva redacción de la CPS, en el que están incluidas implícitamente las Prácticas de Certificación, a los criterios de la AICPA.
- Se procederá al procedimiento descrito en el apartado 11.3 de la presente CPS.
- En su caso, se notificará a los Auditores externos la nueva redacción de la CPS, en el que están incluidas implícitamente las Prácticas de Certificación.
- La Dirección de IPS CERTIFICATION AUTHORITY aprobará la CPS, en el que están incluidas implícitamente las Prácticas de Certificación, con su nueva redacción.
- Se procederá a la publicación en el servidor web de IPS CERTIFICATION AUTHORITY.