

CPS IPS.v2.3 Rev.00

1 de mayo de 2002

CPS de IPS

IPS, S.L.

Edificio ECU

Ctra. de La Coruña, Km. 23,200

28290 - Parque Rozas

(Madrid)

Tel. 91 640 20 52

Fax 91 640 20 41

general@ips.es

<http://www.ips.es>

CPS de IPS

CPS

Versión 2.3

Fecha de Publicación: MAYO de 2002 .

CPS de IPS

© 2002, IPS Internet Publishing Services, 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.

Internet Publishing Services , S.L. (IPS)
CIF B60929452
Edificio ECU
Ctra. De La Coruña, Km. 23,200
28290 – Parque Rozas
(Madrid)
Tel. 91 640 20 52
Fax 91 640 20 41
general@ips.es

Resumen del CPS de IPS

IPS

Edificio ECU

Ctra. De La Coruña, Km. 23,200

28290 – Parque Rozas

(Madrid)

Tel. 91 640 20 52

Fax 91 640 20 41

general@ips.es

<http://www.ips.es>

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

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

IPS también garantiza que cualquier certificado es revocado si en cualquier momento IPS 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 realiza para verificar la información contenida en un certificado se basará en los documentos que se utilizan para comprobar la identidad del suscriptor. En todo caso los trámites efectuados por IPS serán suficientes a los efectos de esta garantía. IPS no da otras garantías.

Responsabilidad

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

Confidencialidad

Los contenidos de los certificados emitidos por IPS son información pública. IPS 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 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 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 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 tiene por objeto el certificar únicamente la información contenida en el mismo. IPS 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 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 o frente a terceros de cualquier declaración incorrecta que hayan hecho a IPS, 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 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 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.

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

En el caso de que IPS 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.

Documento integro

CPS de IPS

Internet Publishing Services , S.L. (IPS)

Edificio ECU

Ctra. de La Coruña, Km. 23,200

28290 - Parque Rozas

(Madrid)

Tel. 91 640 20 52

Fax 91 640 20 41

general@ips.es

www.ips.es

1 INTRODUCCIÓN

1.1 Presentación

IPS, S.L. (en adelante, IPS) **ÚNICAMENTE**, emite Certificados para CA's de Segundo Nivel. La presente CPS, establece las normas, políticas y procedimientos para la emisión de estos Certificados.

Esta Declaración de Prácticas de Certificación (CPS) de IPS está basada en la propuesta del IETF PKIX, de S. Chokhani y W. Ford.

La presente CPS presenta las prácticas de IPS. 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, proporciona 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 están ligadas a sus obligaciones en virtud de sus contratos con IPS.

1.2. Estructura

La estructura de esta CPS es la siguiente:

1 INTRODUCCIÓN

1.1 Presentación.

1.2 Estructura.

1.3 Identificación.

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 Limitaciones de uso de los Certificados.

1.7 Detalles de contacto.

2 ASPECTOS GENERALES.

2.1 Obligaciones.

2.1.1 Obligaciones de IPS.

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 IPS como CA.

2.2.2 Responsabilidad de IPS como AR.

2.2.3 Responsabilidad del suscriptor.

2.2.4 Responsabilidad del usuario.

2.3 Usos de los Certificados de IPS.

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.

2.6.1 Confidencialidad de las claves de firma digital.

2.6.2 Confidencialidad en la prestación de servicios de certificación.

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.

4 GESTIÓN DE LAS CLAVES.

4.1 Aspectos Generales.

4.2 Gestión de las claves de IPS.

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 IPS.

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.**
- 11.4 Procedimiento de aprobación del CPS**

1.3 Identificación

Esta CPS puede ser consultada por Internet en el servidor web de IPS, www.ips.es, o personalmente en las oficinas de IPS.

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

Internet Publishing Services , S.L. (IPS)**CIF B60929452**

**Edificio ECU_
Ctra. de La Coruña, Km. 23,200
28290 - Parque Rozas
(Madrid)
Tel. 91 640 20 52
Fax 91 640 20 41
general@ips.es**

1.4 Comunidad de usuarios y aplicabilidad

La presente CPS **se aplica** a todos los Certificados emitidos por IPS, S.L.. IPS sólo emite Certificados encadenados para otras CA's subordinadas. La presente CPS se aplica a la emisión y uso de Certificados emitidos por IPS, S.L., así como a la CRL de Certificados de IPS, S.L.

1.4.1 Autoridad de Certificación

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

IPS 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 no prevé 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 el único tipo de certificado que se recoge en esta CPS , y cumplir los requisitos que se establezcan en esta CPS. Únicamente podrán ser suscriptores de 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 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, S.L. **ÚNICAMENTE**, emite Certificados para CA's de Segundo Nivel.

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, por lo que son reconocidos técnicamente de forma nativa por los programas de correo, navegadores y servidores web. Una CA de Segundo Nivel se establece mediante un contrato, incluso ante notario en cuanto al cumplimiento de estos compromisos.

1.6. Limitaciones de uso de los Certificados

Los usos autorizados de los Certificados emitidos por IPS están especificados en cada certificado. Todas las personas interesadas podrán consultar estas limitaciones de uso en el propio Certificado Digital.

Las limitaciones de uso podrán ser de cualquier tipo y podrán venir establecidos tanto por IPS, como por el suscriptor o el usuario del certificado. Estas limitaciones quedarán reflejadas, asimismo, en el contrato que se suscriba entre IPS 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.

1.7. Detalles de contacto

Versión del CPS: 2.3
Fecha: 1 de mayo del 2002

Internet Publishing Services , S.L. (IPS)
CIF B60929452

Persona de Contacto: Rodolfo Lomascolo Szittyay
Cargo: Director General

Edificio ECU_
Ctra. de La Coruña, Km. 23,200
28290 - Parque Rozas
(Madrid)
Tel. 91 640 20 52
Fax 91 640 20 41
general@ips.es

2. ASPECTOS GENERALES

2.1 Obligaciones

2.1.1 Obligaciones de IPS

- ?? 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 toda la información necesaria.
- ?? Publicar los certificados emitidos.
- ?? Proteger los datos personales según requerimientos de la LOPD, en su caso.
- ?? Cumplir las obligaciones de la presente CPS.
- ?? 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

La función de AR es realizada por IPS

IPS, en su función de AR, podrá asumir las siguientes obligaciones de las cuales será responsable.

- ?? Identificar y autenticar correctamente al Suscriptor y/o Solicitante y/o a la organización que represente, conforme a los procedimientos que se establecen en esta CPS, utilizando cualquiera de los medios admitidos en derecho.
- ?? Validar las solicitudes de revocación y suspensión.
- ?? Formalizar los contratos de expedición de Certificados con el Suscriptor.

- ?? 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.

2.1.3 Obligaciones del Solicitante

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

2.1.4 Obligaciones del Suscriptor

- ?? 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 Apartado 5 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 IPS 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 IPS acerca de cualquier situación que pueda afectar a la validez del Certificado.
- ?? Destruir el Certificado cuando así lo exija IPS 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.

2.1.5 Obligaciones de los Usuarios

Los Usuarios que pretendan confiar y usar los Certificados emitidos por IPS 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), IPS no se hace responsable del uso y confianza que los Usuarios hagan de estos Certificados.

Los usuarios de Certificados de IPS tienen la obligación de conocer las limitaciones de uso que el Certificado pudiera contener. Los usuarios, para conocer estas limitaciones de uso, deberán consultar el propio Certificado Digital. Además deberán aceptar el régimen de responsabilidad recogido en el Apartado 2.2 de la presente CPS.

2.1.5.1 Confianza en las firmas

Toda persona tendrá derecho a confiar en una firma electrónica emitida mediante un Certificado IPS 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 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 con relación a las firmas emitidas mediante certificados por el emitidos y que se especifican en su CPS.
- ?? Todo otro factor pertinente.

2.1.5.2 Confianza en los certificados

Toda persona tendrá derecho a confiar en un Certificado IPS 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 de IPS con relación a las firmas emitidas mediante certificados por el emitidos y que se especifican en su CPS.
4. Todo otro factor pertinente.

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

2.2 Responsabilidad

2.2.1 Responsabilidad de IPS como CA

IPS 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.

IPS 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 IPS. 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.

IPS 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.

IPS 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 la presente CPS.

IPS 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.

IPS 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 IPS, la pretensión indemnizatoria no podrá exceder, salvo en el supuesto de culpa grave o dolo, la cantidad de 6.000 euros.

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

IPS no es el Agente, Fiduciario ni Administrador o Representante, en ningún caso, de los suscriptores, por lo que no asume ningún tipo de responsabilidad al respecto.

2.2.2 Responsabilidad de IPS como AR

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

IPS 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.

2.2.3 Responsabilidad del Suscriptor

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

2.2.4 Responsabilidad del Usuario

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 IPS por dicho concepto.

2.3 Usos de los Certificados de IPS

Se considerará que se hace un uso indebido de un Certificado cuando éste sea utilizado para realizar operaciones no autorizadas según la CPS y los Contratos de IPS con sus suscriptores.

IPS no asume ninguna responsabilidad por el uso indebido o no autorizado de los Certificados.

2.4 Interpretación y ejecución

2.4.1 Ley aplicable

El presente documento se regirá 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:

IPS 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, IPS 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.

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

IPS notificará de la forma prevista en el párrafo primero del presente apartado a los suscriptores y/o solicitantes de Certificados de IPS en los casos de escisión supervivencia y fusión.

2.4.3 Procedimiento de resolución de conflictos

Para la resolución de cualquier conflicto que pudiera surgir en relación a esta 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

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.

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 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 y los suscriptores de Certificados.

2.5 Publicación y depósito

2.5.1 Publicación de información de IPS

El contenido de esta CPS, así como de toda la información que se publique, estará expuesta a título informativo en el servidor web: <http://www.ips.es> y los originales estarán depositados en las oficinas de IPS.

Igualmente, tanto los Usuarios como los Solicitantes / Suscriptores podrán tener acceso de forma fiable a la información de IPS dirigiéndose a sus oficinas, o bien, solicitándolo a la dirección de correo general@ips.es a través de la cual se remitirá la información firmada con un Certificado de IPS.

No obstante lo señalado en el párrafo anterior, en el servidor web de IPS se encuentra disponible al público información sobre el CPS de IPS, que ésta observa en la emisión de Certificados, su política de precios, la política de privacidad, las condiciones de utilización del servidor web 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

2.6.1 Confidencialidad de las claves de firma digital

Las CA de Segundo Nivel generan y gestionan sus propias claves.

Un responsable de IPS asiste al momento de la generación de las claves de éstos pero, en ningún caso, generará y controlará las claves de la CA de Segundo Nivel. En este caso, una vez generadas las claves de la CA de Segundo Nivel, IPS se obliga a guardar la más absoluta confidencialidad sobre dichas claves.

2.6.2 Confidencialidad en la prestación de servicios de certificación

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

2.7 Derechos de propiedad intelectual

IPS 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 IPS sin la autorización expresa por su parte. No obstante, no necesitará autorización de IPS 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. Auditoría:

2.8.1 Auditorías Internas:

IPS 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, 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 prácticas de certificación.

El Informe de dicha Auditoría determinará sobre la adecuación de las medidas y controles previstas 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 una persona dentro de IPS, S.L., que deberá elevar las conclusiones a la dirección de IPS., S.L. para que adopte las medidas correctoras adecuadas.

En concreto, las áreas que abarca la auditoría encaminadas a comprobar los mecanismos de seguridad en las actividades certificadoras desarrolladas en IPS, 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, S.L..
- ~~///~~ Amenazas físicas externas para IPS, 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, 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, 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, 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:

IPS 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 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, controles de cumplimiento periódicos trimestrales, para determinar con imparcialidad si se siguen cumpliendo, por parte de IPS, los Principios y Criterios WebTrust CA.

Tanto los Informes de las Auditorías, como los Informes de los controles periódicos se comunicarán a la Dirección de IPS 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:

Únicamente podrán ser suscriptores de Certificados de CA de Segundo Nivel personas jurídicas. IPS, S.L. **ÚNICAMENTE**, emite Certificados para CA's de Segundo Nivel. 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.
- 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.

3.1.Certificados para CA de Segundo Nivel:

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.
- Una vez rellena el PCF, el suscriptor y/o solicitante se lo entregará al Responsable autorizado específicamente por IPS 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 IPS:
 - ~~///~~ 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, 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. 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.
 - ✍ 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.
- IPS 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.
 - Antes de que la CA de Segundo Nivel reciba su Certificado de IPS, ésta deberá aprobar el CPS de la CA de Segundo Nivel. Esta aprobación no supone ningún control sobre las actuaciones de la CA de Segundo Nivel respecto a su labor certificadora. Lo que IPS realiza con esta aprobación es comprobar que el CONTENIDO de la CPS de la CA de Segundo Nivel no contradice el CONTENIDO de la CPS de IPS y que la CPS de la CA de Segundo Nivel se ajusta a los principios generales de la CPS de IPS. Por ello, IPS no asume ningún tipo de responsabilidad sobre el cumplimiento que la CA de Segundo Nivel haga de su CPS.
 - IPS 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 en su cuenta corriente. La

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

- Una vez emitido el Certificado por IPS, 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.

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

4 GESTIÓN DE LAS CLAVES:

4.1. Aspectos Generales:

La clave privada de IPS 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 IPS tendrá como objetivo verificar la firma de IPS. En general, IPS seguirá una serie de estándares o normas a la hora de generar el par de claves. Estas normas o estándares son los siguientes:

- El tamaño de las claves será como mínimo de 1024 bits.
- El algoritmo utilizado para la generación de las claves es el RSA.
- El estándar para el módulo criptográfico de generación de claves es el FIPS 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 IPS:

El procedimiento de generación de las claves es el siguiente

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

Las claves de IPS 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.

Existen dos copias de seguridad de la clave de IPS, divididas, cada una de ellas, en dos partes almacenadas cada una de las partes de forma independiente y confidencial, fuera de las instalaciones de IPS.

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:

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

Los suscriptores generan sus claves fuera de las instalaciones de IPS, bajo su responsabilidad, sin el control directo de IPS. Esta generación la pueden realizar mediante dispositivos hardware o software.

IPS 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 IPS 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 IPS 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 del servidor web de IPS.

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 éste 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

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

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 sobrevenida, total o parcial, de cualquiera de ellos, terminación de la representación o extinción de la persona jurídica representada.
- ?? Cese en su actividad de IPS 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 IPS 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 IPS 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.
- ?? La extinción de la CA de Segundo Nivel.

5.1.1 Efectos de la revocación

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

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

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

La revocación del Certificado tendrá como consecuencia la notificación a terceros de que un Certificado ha sido revocado, cuando se solicite la verificación del mismo. Las causas que motivan una revocación es una información no considerada confidencial por IPS, por tal motivo IPS se reserva el derecho de publicarla en la CRL.

5.2 Supuestos de suspensión

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

5.2.1 Efectos y límites de la Suspensión

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

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

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

- ?? Por la decisión de IPS de revocar el Certificado.
- ?? Por decisión de IPS 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

5.3.1 Legitimación activa

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

- ?? El Suscriptor del Certificado así como la persona física o jurídica representada por éste.
- ?? La CA de Segundo Nivel 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 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

La solicitud de suspensión/revocación de Certificados se podrá dirigir a IPS en la forma de comunicación telefónica a través del siguiente número: +34 91 640.20.52

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

Las conversaciones telefónicas que se mantengan con IPS podrán ser grabadas y registradas por IPS a efectos probatorios.

En caso de petición de revocación por parte del suscriptor, un representante de él deberá enviar a la dirección postal de IPS, 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 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 las oficinas de IPS.

5.3.3 Decisión de suspender/revocar

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

IPS 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

La decisión de suspender/revocar el Certificado será comunicada por IPS 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 IPS, salvo que la causa de revocación sea el cese de la actividad de IPS, en cuyo caso, la pérdida de eficacia tendrá lugar desde que esa circunstancia se produzca.

6 CADUCIDAD DE CERTIFICADOS

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

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

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

7 RENOVACIÓN DE LOS SERVICIOS DE CERTIFICACIÓN

7.1 Renovación de Certificados

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

En este caso, IPS 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 hace 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 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 si concurren los extremos generales que a continuación se detallan.

7.1.1 Requisitos previos

Deberán concurrir los siguientes:

- ?? IPS 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 la fecha 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 especifica a tal efecto.

- ?? Que IPS no haya tenido conocimiento cierto de la concurrencia de ninguna causa de revocación/suspensión del certificado.

- ?? 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

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

El suscriptor enviará ese formulario debidamente cumplimentado a IPS 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.

IPS procederá a la verificación y validación de la identidad del suscriptor que ha solicitado la renovación de su Certificado.

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.

7.1.3 Procedimiento de renovación de certificados

Cuando IPS reciba la solicitud del suscriptor en debida forma, éste **procederá a la generación de nuevas claves criptográficas** e IPS 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.

IPS comunicará 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 IPS para recogerlo 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 IPS según se establece en los correspondientes contratos y la CPS.

7.2 Reemisión de certificados

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 del CPS)

7.3. Regeneración de claves:

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

8 EXTINCIÓN DE IPS

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

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

9 CONTROLES DE SEGURIDAD

9.1 Manual Interno de Seguridad

Con el objeto de reforzar la seguridad técnica, física, de procedimientos y de capacitación del personal, IPS dispone de un Manual Interno de Seguridad que regula todos estos aspectos. En el mencionado Manual se encuentran definidas una serie de medidas para garantizar los aspectos señalados. Algunas de estas medidas se encuentran implementadas y otras se implementarán en el plazo de tiempo más breve posible. 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 medidas que, actualmente, se encuentran implementadas en IPS referentes a su labor certificadora.

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. 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.

IPS realiza un inventario de todo el hardware dedicado a la labor certificadora. En el mencionado inventario se especifica la marca, el modelo, el número de serie y otras cuestiones características del mencionado hardware.

IPS realiza un inventario de todo el software dedicado a la labor certificadora. En el mencionado inventario se especifica la versión y, en general, todas aquellas cuestiones características del mismo.

9.3. Seguridad del Personal.

Todos los empleados de IPS firman un acuerdo de confidencialidad con la empresa.

Los empleados de IPS dedicados a la labor certificadora, reciben el correspondiente adiestramiento para acometer dicha labor.

9.4. Seguridad física y del entorno.

El equipo para el proceso de la información que alberga la CA de IPS se encuentra offline en un lugar fuera de las instalaciones de IPS 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 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:

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

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

Los soportes en los que se contienen las copias de seguridad de la clave privada de IPS están ubicados en un lugar, ubicado a menos de 600 kilómetros de las oficinas de IPS, tal que, en caso de desastre como, por ejemplo, incendio o inundaciones, en la oficina principal de IPS, escaparían de los daños que pudieran sufrir.

IPS dispone de un procedimiento 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.

IPS 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 IPS 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 IPS.

Los ordenadores y terminales de IPS y, en especial, los que se dediquen a la labor certificadora de IPS, 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.

9.6. Seguridad para usuarios de sistemas

Los usuarios, es decir, los empleados de IPS han recibido formación e instrucciones 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.
- El uso de programas.
- 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.

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

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

9.8 Incidencias

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.
- ~~///~~ Accesos no autorizados a lugares dónde se ubican los sistemas informáticos.
- ~~///~~ Registro de entradas de sesión denegadas
- ~~///~~ Cualquier otra anomalía que afecte o pudiera afectar a la seguridad de los datos o al acceso de las distintas plataformas informáticas.

IPS 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.

9.9. Cumplimiento.

Todo el software utilizado en IPS y, en especial el referido a la labor certificadora de IPS 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.

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 ha elaborado e implementado un Documento de Seguridad.

10 CARACTERÍSTICAS DE LOS CERTIFICADOS Y DE LAS LISTAS DE CERTIFICADOS

10.1 Características del Certificado

El Certificado 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 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.

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

10.2 Listas de Certificados

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

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

El Listado de Certificados en Vigor estará a disposición de los usuarios en el servidor web de IPS.

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

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 IPS durante un periodo de doce años.

La CRL se publica una vez al mes en el servidor web de IPS. 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 91 640.20.52

El contenido de las CRL's publicadas por IPS 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.

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

IPS podrá modificar las estipulaciones de la presente 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.

Las modificaciones efectuadas sobre la CPS, de acuerdo a lo establecido en el apartado 11.4 de la presente CPS, no existe en el índice se darán a conocer a los interesados en la página web de IPS www.ips.es y en las oficinas de IPS.

11.3 Procedimiento de notificación de las publicaciones

En caso que las modificaciones efectuadas en la 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, realizadas por IPS, 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, se procederá de la siguiente forma:

- Se procederá a la modificación de los apartados específicos en el CPS original.
- Se verificará las posibles relaciones de los textos modificados, en relación con la CPS completo.
- Se procederá a comprobar la adecuación de la nueva redacción de la CPS, 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.
- La Dirección de IPS aprobará la CPS con su nueva redacción.
- Se procederá a la publicación en el servidor web de IPS.