

Política de Certificados
PSC World, S.A. de C.V.
Prestador de Servicios de Certificación



Tabla de Contenido

1. Introducción.....	3
1.1 Alcance.....	3
SECRETARIA DE ECONOMIA.....	3
SECRETARIA DE COMERCIO Y FOMENTO INDUSTRIAL.....	4
1.2 Definiciones.....	4
2. Comunidad de usuarios y utilización de los certificados.....	5
3. Obligaciones.....	6
3.1. Obligaciones de PSC World como Agencia Certificadora.....	6
3.2. Obligaciones de PSC World como Agencia Registradora.....	6
3.3. Obligaciones de los Agentes Certificadores acreditados por PSC World.....	7
3.4. Obligaciones de los Solicitantes y Titulares de certificados.....	7
3.5. Obligaciones de PSC World y sus entidades acreditadas.....	8
3.6. Exclusiones de responsabilidad.....	9
3.6.1 Exclusión de responsabilidades de la Autoridad Certificadora.....	9
3.6.2 Exclusión de responsabilidades de la Autoridad Registradora.....	9
4. Requerimientos Operacionales.....	10
4.1. Interoperatividad.....	10
4.2. Procedimiento de Operación para Otorgar Certificados.....	10
4.3. Circunstancia de revocación de un certificado.....	11

1. Introducción

Una política de certificado está definida, según el estándar internacional “ISO/IEC 9594-8/ITU-T Recomendación X.509”, como “un conjunto de reglas que indican la aplicabilidad de un certificado a una comunidad en particular y/o clase de aplicación con requerimientos de seguridad comunes”.

PSC World tiene como objetivo la implementación de los Servicios de Seguridad Administrado para la Infraestructura de Llave Pública (PKI), a partir de una revisión metodológica acorde a las mejores prácticas internacionales en materia de Seguridad de la Información y la aplicación de las leyes y normativas existentes en México. Para ofrecer este servicio **PSC World** se convierte en su ***Prestador de Servicios de Certificación.***

PSC World, en su deseo de promover la transparencia y calidad de los certificados que emite, ha adoptado criterios internacionalmente reconocidos en la definición, estructura y presentación de esta Política de Certificados, tales como el estándar ETSI TS 102 042 y asegura su concordancia con la Declaración de Prácticas de Certificación y los procedimientos operacionales.

¿Qué es un Prestador de Servicios de Certificación?

Es una persona física o institución pública que presta servicios relacionados con Firmas Electrónicas y expide certificados, actuando como tercera parte de confianza entre las personas u organizaciones que intercambian mensajes utilizando firma electrónica.

[← Regresar](#)

1.1 Alcance

Esta *Política de Certificados*, en conjunto con la *Declaración de Prácticas de Certificación*, son los únicos instrumentos que establecen las reglas aplicables para la solicitud, validación, aceptación, entrega, emisión y revocación de los certificados, así como las restricciones y aplicaciones en las cuales se deben utilizar dichos certificados

Una explicación detallada de las prácticas que **PSC World** emplea para emitir y gestionar certificados, y que implementa y soporta los requerimientos de estas políticas de certificado, se encuentra en el documento *Declaración de Prácticas de Certificación.*

En esta *Política de Certificados* se podrá encontrar las reglas y procedimientos que dan cumplimiento a:

SECRETARIA DE ECONOMIA

- DECRETO por el que se reforman y adicionan diversas disposiciones del Código de Comercio en materia de Firma Electrónica; publicado en el Diario Oficial el 29 de agosto de 2003
- REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación; publicado en el Diario Oficial el 19 de julio de 2004
- REGLAS generales a las que deberán sujetarse los Prestadores de Servicios de Certificación; publicado en el Diario Oficial el 10 de agosto de 2004

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 3 de 12

SECRETARIA DE COMERCIO Y FOMENTO INDUSTRIAL

- DECRETO por el que se reforman y adicionan diversas disposiciones del Código Civil para el Distrito Federal en Materia Común y para toda la República en Materia Federal, del Código Federal de Procedimientos Civiles, del Código de Comercio y de la Ley Federal de Protección al Consumidor; publicado en el Diario Oficial el 19 de mayo de 2000

Tales políticas son las que se prosigue en detallar, y están disponibles en el Sitio WEB de PSC World (www.pscworld.com) para conocimiento público.

[← Regresar](#)

1.2 Definiciones

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.

Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.

Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.

Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.

Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.

Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.

En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.

Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.

Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.

Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

Secretaría: Se entenderá la Secretaría de Economía.

Prestador de Servicios de Certificación: La persona o institución que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.

Solicitante: Se entenderá a la persona que tramita la Solicitud de Certificado

Titular: Se entenderá a la persona a cuyo favor fue expedido el Certificado.

Agente Certificador: A la institución o persona física que verifica la identidad de los Solicitantes

Agencia Certificadora: A la institución que presta servicios de certificación mediante la expedición de Certificados Digitales

Agencia Registradora: A la institución autorizada para llevar el registro electrónico de los Certificados Digitales expedidos por la Agencia Certificadora.

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 4 de 12

[← Regresar](#)

2. Comunidad de usuarios y utilización de los certificados

Los certificados emitidos por **PSC World** se emiten a personas físicas y organizaciones públicas o privadas. En el primer caso se asegura la identidad del suscriptor requiriendo su presencia física ante un Agente Certificador. En el caso de una organización, se asegura la existencia y nombre mediante el cotejo de los datos registrados con los contenidos en bases de datos independientes, estos certificados podrán ser utilizados para soportar las siguientes necesidades de seguridad:

Autenticación: proporciona suficientes garantías respecto a la identidad del suscriptor del certificado, al requerirse la presentación en persona del Solicitante junto con los documentos establecidos en el *Requerimiento de Solicitud de Certificado Digital* que acreditan su personalidad.

Integridad de mensajes: los mensajes firmados con identidades digitales de clase 3, permiten validar si el contenido de un mensaje de datos ha sido alterado en el tiempo transcurrido entre su envío y su recepción efectiva.

Firmas digitales: las firmas digitales producidas con identidades de clase 3, ofrecen los medios de respaldo frente a que una persona deniegue de la autoría y contenido de un mensaje de datos en particular, sí la persona ha firmado digitalmente dicho mensaje.

Privacidad: las identidades digitales de clase 3 permiten cifrar mensajes de forma que al ser transmitidos sean solo observados por el remitente correspondiente.

Los certificados emitidos por **PSC World** podrán ser utilizados para:

Certificado de Servidor - El certificado tendrá como única finalidad asegurar la existencia y denominación de una entidad en Internet. Estos certificados serán utilizados a través de aplicaciones en servidores con protocolo SSL (Secure Socket Layer).

Representación de empresas – El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas con actividad empresarial o personas morales para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes, así como que el representante legal de una empresa manifieste que su representada se encuentra capacitada legalmente para la celebración del acto y acreditar que la personalidad que ostenta y las facultades con que cuenta no le han sido limitadas, modificadas o revocadas.

Certificado personal - El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes.

Certificado de Correo Electrónico – El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar ante terceros su identidad, autenticidad e integridad de los mensajes mediante aplicaciones de correo electrónico seguro S/MIME, para cifrar y firmar mensajes.

[← Regresar](#)

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 5 de 12

3. Obligaciones

3.1. Obligaciones de PSC World como Agencia Certificadora

- a. Cumplir con los requisitos establecidos en el **REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación**, publicado en el Diario Oficial el 19 de Julio de 2004
- b. Cumplir con los requisitos establecidos en las **REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación**, publicado en el Diario Oficial el 10 de Agosto de 2004
- c. Emitir Certificados Digitales que cumplan al menos con los requisitos previstos
- d. Revocar los Certificados Digitales al cumplirse cualquiera de los **Circunstancias de Revocación de Certificados** previstas.
- e. Proporcionar al solicitante de un Certificado Digital, los medios necesarios para que genere sus datos de creación de Firma Electrónica y datos de verificación de Firma Electrónica, en forma secreta y bajo su total control.
- f. Hacer del conocimiento del solicitante sus derechos y obligaciones, como Titular de un Certificado Digital.
- g. Recibir los precertificados y validar la firma electrónica de los Agentes Certificadores y de los Solicitantes.
- h. Enviar los certificados a las Agencias Registradoras para su registro.
- i. Enviar los certificados ya registrados en la Agencia Registradora y al Agente Certificador para que a su vez entregue el recibo de emisión al Titular
- j. Crear los certificados digitales de los Agentes Certificadores y/o acreditarlos como tales.
- k. Generar las Listas de Revocación
- l. Hacer las funciones de Agente Certificador cuando sea necesario.
- m. Ejecutar todas las actividades que le correspondan de acuerdo a la **Declaración de Prácticas de Certificación**

[← Regresar](#)

3.2. Obligaciones de PSC World como Agencia Registradora.

- a. Cumplir con los requisitos establecidos en el **REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación**, publicado en el Diario Oficial el 19 de Julio de 2004
- b. Cumplir con los requisitos establecidos en las **REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación**, publicado en el Diario Oficial el 10 de Agosto de 2004
- c. Registrar certificados digitales siempre y cuando la Agencia Registradora Central confirme la unicidad de las llaves públicas.
- d. Administrar las bases de datos con los certificados digitales registrados, tanto actuales como históricas.
- e. Permitir la consulta en línea por medio electrónico del estado de los Certificados Digitales por ella registrados.
- f. Proporcionar los certificados digitales que le soliciten los Solicitantes a través de medios electrónicos.

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 6 de 12

- g. Divulgar la Lista de Revocaciones.
- h. Garantizar la integridad de las Listas de Revocación
- i. Conservar toda la información y documentación relativa a los certificados
- j. Ejecutar todas las actividades que le correspondan de acuerdo a la ***Declaración de Prácticas de Certificación***

[← Regresar](#)

3.3. Obligaciones de los Agentes Certificadores acreditados por PSC World

- a. Verificar la identidad de los Solicitantes que desean obtener certificados digitales.
- b. Verificar y corroborar la información contenida en el ***Requerimiento de Solicitud de Certificado Digital*** con base en los documentos solicitados
- c. Garantizar que el Solicitante cumpla con los requisitos establecidos en la ***Declaración de Prácticas de Certificación***
- d. Procesar los requerimientos de certificación
- e. Ejecutar todas las actividades que le correspondan de acuerdo a la ***Declaración de Prácticas de Certificación***
- f. Los Agentes Certificadores responderán ante **PSC World** por los daños y perjuicios que pudieran derivarse de la ejecución de sus obligaciones concertadas de manera negligente o en forma distinta a la contemplada en la ***Declaración de Prácticas de Certificación***

[← Regresar](#)

3.4. Obligaciones de los Solicitantes y Titulares de certificados.

- a. Establecer su frase de seguridad y generar su par de claves (pública y privada).
- b. Solicitar su certificado digital a través de un Agente Certificador o Fedatario, presentando su ***Requerimiento de Solicitud de Certificado Digital***
- c. Conocer y aceptar las normas estipuladas en el contrato con **PSC World**
- d. Descargar su certificado digital ya registrado.
- e. Mantener en un lugar seguro su clave privada.
- f. No olvidar la frase de seguridad y mantenerla en secreto.
- g. Notificar a **PSC World** de cualquier modificación de sus antecedentes, que como consecuencia pudiera invalidar uno o más certificados emitidos a su nombre.
- h. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;
- i. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma
- j. Cuando se emplee un Certificado en relación con una Firma Electrónica, actuar con diligencia razonable para cerciorarse de que todas las declaraciones que haya hecho en relación con el Certificado, con su vigencia, o que hayan sido consignadas en el
- k. Ejecutar todas las actividades que le correspondan de acuerdo a la ***Declaración de Prácticas de Certificación***

[← Regresar](#)

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 7 de 12

3.5. Obligaciones de PSC World y sus entidades acreditadas

- a. Contar con los elementos humanos, materiales, económicos y tecnológicos que garanticen su operación.
- b. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante
- c. Poner a disposición del Firmante los dispositivos de generación de los Datos de Creación y de verificación de la Firma Electrónica
- d. Informar, antes de la emisión de un Certificado, a la persona que solicite sus servicios, de su precio, de las condiciones precisas para la utilización del Certificado, de sus limitaciones de uso y, en su caso, de la forma en que garantiza su posible responsabilidad.
- e. Mantener un registro de Certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión, pérdida o terminación de vigencia de sus efectos. A dicho registro podrá accederse por medios electrónicos, ópticos o de cualquier otra tecnología y su contenido público estará a disposición de las personas que lo soliciten, el contenido privado estará a disposición del Destinatario y de las personas que lo soliciten cuando así lo autorice el Firmante, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría;
- f. Guardar confidencialidad respecto a la información que haya recibido para la prestación del servicio de certificación;
- g. En el caso de cesar en su actividad, los Prestadores de Servicios de Certificación deberán comunicarlo a la Secretaría a fin de determinar, conforme a lo establecido en las reglas generales expedidas, el destino que se dará a sus registros y archivos;
- h. Asegurar las medidas para evitar la alteración de los Certificados y mantener la confidencialidad de los datos en el proceso de generación de los Datos de Creación de la Firma Electrónica;
- i. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el Destinatario,
- j. Proporcionar medios de acceso que permitan a la Parte que Confía en el Certificado determinar:
 - i. La identidad del Prestador de Servicios de Certificación;
 - ii. Que el Firmante nombrado en el Certificado tenía bajo su control el dispositivo y los Datos de Creación de la Firma en el momento en que se expidió el Certificado;
 - iii. Que los Datos de Creación de la Firma eran válidos en la fecha en que se expidió el Certificado;
 - iv. El método utilizado para identificar al Firmante;
 - v. Cualquier limitación en los fines o el valor respecto de los cuales puedan utilizarse los Datos de Creación de la Firma o el Certificado;
 - vi. Cualquier limitación en cuanto al ámbito o el alcance de la responsabilidad indicada por el Prestador de Servicios de Certificación;

- vii. Si existe un medio para que el Firmante dé aviso al Prestador de Servicios de Certificación de que los Datos de Creación de la Firma han sido de alguna manera controvertidos, y
- viii. Si se ofrece un servicio de terminación de vigencia del Certificado.

[← Regresar](#)

3.6. Exclusiones de responsabilidad

3.6.1 Exclusión de responsabilidades de la Autoridad Certificadora

- a. PSC World no será responsable de cualquier daño o perjuicio que se derive de utilizaciones negligentes o dolosas no acorde con las políticas establecidas en esta *Política de Certificado* y la *Declaración de Prácticas de Certificación* por parte de de los usuarios y/o titulares de Certificados Digitales.
- b. PSC World no responderá de la utilización del certificado para usos distintos de aquellos para los cuales se haya emitido.
- c. PSC World no será responsable del contenido de los documentos firmados digitalmente ni de las páginas Web que contengan un certificado por ella emitido.
- d. PSC World no será responsable de cualquier daño o perjuicio por el no cumplimiento del *Acuerdo de Prestación de Servicios* por parte de los usuarios y/o titulares de Certificados Digitales.

[← Regresar](#)

3.6.2 Exclusión de responsabilidades de la Autoridad Registradora

- a. PSC World no será responsable de cualquier tipo de daños o perjuicios que sufran sus usuarios y/o titulares de Certificados Digitales, siempre que estos se deriven de la mala o indebida utilización de los servicios por parte de dichos usuarios y/o titulares de Certificados Digitales.
- b. PSC World tampoco será responsable frente a terceros afectados, que tengan una relación directa o indirecta con los servicios que presta la Autoridad Registradora.
- c. PSC World no será responsable por los daños y/o perjuicios de cualquier naturaleza como pueden ser de manera enunciativa más no limitativa, pérdida de utilidades, suspensión de operaciones, pérdida de información comercial o cualquier otro daño monetario; si éstos son causados por la mala o indebida utilización de los servicios por parte de los usuarios y/o titulares de Certificados Digitales.
- d. PSC World no será responsable por los daños y/o perjuicios de la errónea interpretación, análisis, síntesis o conclusión a que los usuarios y/o titulares de Certificados Digitales lleguen en el uso de los servicios.
- e. PSC World no será responsable por los daños y/o perjuicios que se causen, si el solicitante de un Certificado Digital aporta datos o documentos falsos, para la obtención de dicho certificado.
- f. No será responsable por la interrupción o alteración temporal de los servicios por causas ajenas a la Agencia Registradora, como pueden ser de manera enunciativa más no limitativa, condiciones climatológicas adversas, sismos, inundaciones, fallas en la energía eléctrica, fuego, actos vandálicos, huelga, o cualquier otro motivo que afecte sus instalaciones.

- g. No será responsable por la interrupción temporal de los servicios que presta la Agencia Registradora, cuando deriven de situaciones realizadas por las autoridades competentes que limiten la libertad en las comunicaciones.
- h. PSC World no será responsable de cualquier daño o perjuicio por el no cumplimiento del *Acuerdo de Prestación de Servicios* por parte de los usuarios y/o titulares de Certificados Digitales.

[← Regresar](#)

4. Requerimientos Operacionales

4.1. Interoperatividad

- a. PSC World garantiza la interoperatividad de los certificados a través del cumplimiento de las disposiciones emitidas por la Secretaria
- b. PSC World a través de su aliado tecnológico SeguriData Privada S.A. de C.V., garantiza el cumplimiento de los siguientes estándares:
 - i. Estructura de datos del certificado compatible con el estándar ISO/IEC 9594-8; además de contener los datos que aparecen en el artículo 108 del Código de Comercio.
 - ii. Los algoritmos utilizados para la Firma Electrónica Avanzada será compatibles con los estándares de la industria RFC 3280. Internet X509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (Obsoletes 2459), R. Housley, W. Polk, W. Ford, D. Solo, April 2002, o los que les sustituyan que provean un nivel adecuado de seguridad tanto para la firma del Prestador de Servicios de Certificación como del usuario.
 - iii. Estructura e información de la Lista de Certificados Revocados compatible con la última versión del estándar ISO/IEC 9594-8 o la que le sustituya.
 - iv. En el caso de las claves utilizadas para la generación de una Firma Electrónica Avanzada, su tamaño proveerá un nivel de seguridad de 1024 bits para los usuarios y de 2048 bits para PSC World y utilizarán funciones hash conforme a los estándares de la industria, además de proveer el adecuado nivel de seguridad para este tipo de firmas tanto de PSC World como del usuario.

[← Regresar](#)

4.2. Procedimiento de Operación para Otorgar Certificados

- a. Los procedimientos de operación para otorgar certificados digitales quedan descritos en la *Declaración de Prácticas de Certificación*.
- b. El proceso se puede describir en las siguientes subprocesos
 - i. Proceso de Registro del Solicitante: En este proceso el solicitante realiza vía Internet su Requerimiento de Solicitud de Certificado y genera su par de llaves
 - ii. Proceso de acreditación de la personalidad del Solicitante: En este proceso el solicitante se presenta ante un Agente Certificador y acredita su personalidad.
 - iii. Proceso de Certificación de la identidad del Solicitante: En este proceso el Agente Certificador, acredita la personalidad del Solicitante y procesa el Requerimiento de Solicitud de Certificado
 - iv. Proceso de Generación del Certificado Digital: En este proceso la Agencia Certificadora emite el Certificado Digital

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 10 de 12

- c. PSC World para la Prestación de los Servicios de Certificación cuenta con una alianza con SeguriData Privada S.A. de C.V. que le permite utilizar como solución tecnológica sus productos:
 - i. SeguriServer: Este producto proporciona servicios de Agencia Certificadora e incluye además las funciones de Agencia Registradora, permitiendo la emisión y administración de los certificados digitales.
- d. PSC World, se reserva el derecho a solicitar cualquier información adicional al Solicitante o a terceros, que permita la verificación de las circunstancias que habrán de constar en el certificado.
- e. PSC World, se reserva el derecho a no emitir certificados cuando así lo estime conveniente, comunicando las razones de la negación, sin que por ello pueda exigirse responsabilidad alguna
- f. PSC World garantiza poner a disposición del Solicitante los dispositivos de creación y validación de la firma electrónica
- g. PSC World deja claramente establecido que no comparte, vende, cede, ni transfiere la información personal de los usuarios.

[← Regresar](#)

4.3. Circunstancia de revocación de un certificado

Un Certificado dejará de surtir efectos para el futuro, en los siguientes casos:

- a. Condiciones para la revocación por el Prestador de Servicios de Certificación
 - Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido.
 - Por haberse comprobado que al momento de su expedición, el Certificado no cumplió con los requisitos establecidos en la ley, situación que no afectará los derechos de terceros de buena fe.
 - Resolución judicial o de autoridad competente que lo ordene.
 - Cuando se haya producido un error en la emisión del certificado debido a una falta de adecuación en el procedimiento establecido
 - Cuando el Solicitante incumpla las condiciones de utilización de los certificados establecidas en el contrato con **PSC World**
- b. Condiciones para la revocación por el Prestador de Servicios de Certificación a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado, o a través del **Servicio de Certificación vía Web** por el Firmante antes de que concluya el periodo de vigencia del Certificado
 - Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado.
 - Cuando la seguridad de la clave privada se haya comprometido

PSC World establece en su **Declaración de Prácticas de Certificación** los procedimientos para solicitar la suspensión o revocación de un certificado

Una vez recibida la solicitud de revocación en **PSC World** esta es procesada generándose inmediatamente la revocación efectiva del certificado correspondiente,

Documento: Política de Certificados	Número: POL002-01SE
Propietario: PSC World	Versión 1.01/010804
	Página 11 de 12

Para brindar un adecuado servicio de información sobre las revocaciones y suspensiones, PSC World soportará 3 medios para distribuir dicha información, las cuales se detallan en ***la Declaración de Prácticas de Certificación***

Las listas de Certificados Revocados serán actualizadas con una frecuencia de 12 horas entre cada publicación.

[← Regresar](#)