

# Política de Certificados PSC World

---

## Tabla de Contenido

1.	INTRODUCCIÓN.....	2
1.1.	Sobre la Política de Certificados.....	2
1.2.	Alcance.....	2
1.3.	Referencias.....	2
1.4.	Definiciones.....	2
1.5.	Comunidad de usuarios y utilización de los certificados.....	3
1.5.1.	Comunidad de usuarios.....	3
1.5.2.	Tipos y usos de los certificados.....	3
1.5.3.	Tipos de acreditación de la identidad y/o personalidad.....	4
1.6.	Contacto.....	4
2.	OBLIGACIONES Y RESPONSABILIDADES.....	5
2.1.	Obligaciones de PSC World como Agencia Certificadora.....	5
2.2.	Responsabilidades de PSC World como Agencia Certificadora.....	5
2.3.	Exclusión de responsabilidades PSC World como Agencia Certificadora.....	6
2.4.	Obligaciones de PSC World como Agencia Registradora.....	6
2.5.	Responsabilidades de PSC World como Agencia Registradora.....	6
2.6.	Exclusión de responsabilidades de PSC World como Agencia Registradora.....	6
2.7.	Obligaciones de los Agentes Certificadores.....	7
2.8.	Responsabilidades de los Agentes Certificadores.....	7
2.9.	Exclusión de responsabilidades de los Agentes Certificadores.....	7
2.10.	Obligaciones y responsabilidades de los Solicitantes y Titulares de certificados.....	7
2.11.	Responsabilidades de los Solicitantes y Titulares de certificados.....	7
2.12.	Responsabilidades de la Parte que Confía.....	8
3.	IDENTIFICACIÓN Y AUTENTICACIÓN.....	8
3.1.	Método de verificación de identidad del solicitante.....	8
3.2.	Convenciones de nombre.....	9
3.2.1.	DN (Distinguished Names) de la Agencia Certificadora PSC World.....	9
3.2.2.	DN (Distinguished Names) de los certificados emitidos.....	10
3.3.	Revocación de certificados.....	10
3.3.1.	Periodo de validez de los certificados digitales.....	10
3.3.2.	Método de verificación del Titular.....	10
4.	REQUERIMIENTOS OPERACIONALES.....	10
4.1.	Procedimiento de Operación para Otorgar Certificados.....	10
4.2.	Circunstancia de revocación de un certificado.....	10
4.3.	Distribución de certificados.....	11
4.4.	Publicación de información de revocaciones.....	11
4.5.	Frecuencia de actualización de la Lista de Certificados Revocados.....	11
4.6.	Auditoria.....	11
5.	PRIVACIDAD Y SEGURIDAD.....	12
5.1.	Requerimientos de Seguridad de la Agencia Certificadora PSC World.....	12
5.2.	Requerimientos de Privacidad de la Agencia Certificadora PSC World.....	12
6.	INTEROPERATIVIDAD.....	12

## 1. INTRODUCCIÓN

**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**.

*¿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.

**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**, que asegura su concordancia con la **Declaración de Prácticas de Certificación** y los procedimientos operacionales.

### 1.1. Sobre la Política de Certificados

Una política de certificados 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".

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 esta **Política de certificados**, se encuentra en el documento **Declaración de Prácticas de Certificación**.

### 1.2. Alcance

Describir la **Política de Certificados** de la **Agencia Certificadora PSC World**, dentro de la Infraestructura de Llaves Públicas (PKI) de **PSC World**.

La **Agencia Certificadora PSC World** se establece para desarrollar y crear una infraestructura de llave pública a nivel nacional para el desarrollo del comercio electrónico; podrá certificar:

- Las claves públicas de personas físicas o morales.
- Las claves públicas de los Agentes Certificadores

### 1.3. Referencias

- ETSI TS 102 042 v1.1.1- Policy requirements for certification authorities issuing public key certificates, abril 2002
- RFC 3647 - Internet X509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, noviembre 2003
- RFC 3280 - Internet X509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile abril 2002
- 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.

### 1.4. 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.

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 2 de 12

**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.

## **1.5. Comunidad de usuarios y utilización de los certificados**

### **1.5.1. Comunidad de usuarios**

**PSC World** emite Certificados Digitales basados en la estándar ITU-T Recommendation X.509 para sus Agentes Certificadores, personas físicas y organizaciones públicas o privadas.

Para el **Agente Certificador**, asegura la identidad del suscriptor, requiriendo su presencia física ante el Oficial de Seguridad de PSC World

Para personas físicas, 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.

### **1.5.2. Tipos y usos de los certificados**

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

1. **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)
2. **Certificado de Representación** – 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

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 3 de 12

no le han sido limitadas, modificadas o revocadas.

3. **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.

A continuación se muestra un resumen de los tipos de certificados emitidos por **PSC World**.

<b>Descripción de tipos de Certificados</b>		
<b>Tipo</b>	<b>Características generales</b>	<b>Usos típicos</b>
Certificado de Servidor	<ul style="list-style-type: none"> <li>▪ Requiere presencia personal de la persona física o un representante legal de la empresa para acreditar la personalidad de la representada</li> <li>▪ Validación de identidad del servidor con autoridades de registro de nombres de dominio</li> <li>▪ Se registra documentación y firma autógrafa</li> <li>▪ Certificados SSL de 128 bits</li> </ul>	<ul style="list-style-type: none"> <li>▪ Autenticación de servidor</li> <li>▪ Comercio electrónico</li> </ul>
Certificado de Representación	<ul style="list-style-type: none"> <li>▪ Requiere presencia personal de la persona física o un representante legal de la persona moral para acreditar la personalidad de la representada</li> <li>▪ Se registra documentación y firma autógrafa</li> <li>▪ Certificado de 1024 bits</li> </ul>	<ul style="list-style-type: none"> <li>▪ Comercio electrónico</li> <li>▪ Servicios de suscripción</li> <li>▪ Correo electrónico seguro S/MIME</li> <li>▪ Autenticación en sitio Web</li> <li>▪ Firma de documentos</li> <li>▪ Firma de contratos</li> </ul>
Certificado personal	<ul style="list-style-type: none"> <li>▪ Requiere presencia personal para acreditar la identidad</li> <li>▪ Se registra documentación y firma autógrafa</li> <li>▪ Certificado de 1024 bits</li> </ul>	<ul style="list-style-type: none"> <li>▪ Comercio electrónico</li> <li>▪ Servicios de suscripción</li> <li>▪ Correo electrónico seguro S/MIME</li> <li>▪ Autenticación en sitio Web</li> <li>▪ Firma de documentos</li> <li>▪ Firma de contratos</li> </ul>

Todos los Certificados emitidos por PSC World tienen el mismo nivel de Seguridad.

### 1.5.3. Tipos de acreditación de la identidad y/o personalidad.

La acreditación de la identidad y/o personalidad del **Solicitante** para la emisión del certificado, es realizada por un **Agente Certificador**. **PSC World** contempla dos tipos de certificación posible para cada tipo de certificado:

1. **Con Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante.
2. **Sin Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante.

#### Características:

**Con Fe Pública:** Son acreditados por un Fedatario Público autorizado como **Agente Certificador** de **PSC World** y son registrados con Ratificación de Firma, por lo tanto son instrumentos públicos en los términos de los artículos 1237 y 1391 fracción II del código de comercio. (Permite la equivalencia del papel ante un juzgado).

**Sin Fe Pública:** Son acreditados ante un **Agente Certificador** de **PSC World**.

### 1.6. Contacto

Cualquier consulta respecto a las normas contenidas en este documento, puede ser realizada al Oficial de Seguridad, en la siguiente dirección:

**PSC World S.A. de C.V.**  
 Elena 359, Colonia Nativitas  
 Delegación Benito Juárez  
 México, Distrito Federal  
 Código Postal 03500

**Teléfono:** (52)-(55)-56989898

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 4 de 12

e-mail: [servicios@pscworld.com.mx](mailto:servicios@pscworld.com.mx)

Web: <http://www.pscworld.com>

## 2. OBLIGACIONES Y RESPONSABILIDADES

### 2.1. Obligaciones de PSC World como Agencia Certificadora

- a. Contar con los elementos humanos, materiales, económicos y tecnológicos que garanticen la seguridad y operación de los servicios.
- b. Mantener en todo momento protegido sus datos de Creación de Firma Electrónica
- c. Prestar servicios de certificación mediante la expedición de Certificados Digitales
- d. Aprobar o denegar las Solicitudes de Certificados.
- e. Emitir Certificados Digitales que cumplan al menos con los requisitos previstos en el Código de Comercio.
- f. Revocar los Certificados Digitales al cumplirse cualquiera de los **Circunstancias de Revocación de Certificados** previstas.
- g. Generar y publicar la Lista de Certificados Revocados.
- a. Enviar copia de cada certificado emitido a la Agencia Certificadora Raíz de la Secretaría de Economía, de acuerdo a lo establecido en el capítulo 5 de las **REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación** así como copia de cada publicación de la Lista de Certificados Revocados.
- b. Publicar los certificados emitidos en su sitio Web para consulta de cualquier usuario.
- h. Permitir la consulta en línea de su Certificado.
- i. 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.
- j. Hacer del conocimiento del solicitante sus derechos y obligaciones, como Titular de un Certificado Digital, mismo que se especifica en el **Acuerdo de Prestación de Servicios**
- k. Notificar inmediatamente a toda la cadena de certificación, el compromiso de sus **Datos de Creación de Firma Electrónica**, con el objetivo de revocar y volver a generar el par de llaves de cada **Titular**.
- l. En el caso de cesar en su actividad, 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.
- m. No emitir certificados con una duración superior a la vigencia de su vínculo administrativo con el **Solicitante**.
- n. Contar con los elementos humanos, materiales, económicos y tecnológicos que garanticen la seguridad y operación de los servicios.
- o. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el destinatario.
- p. Proteger los datos de carácter personal suministrados por el **Solicitante**.
- q. Ejecutar todas las actividades que le correspondan de acuerdo a la **Declaración de Prácticas de Certificación**.

### 2.2. Responsabilidades de PSC World como Agencia Certificadora

- a. 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.
- b. 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.

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 5 de 12

- vii. 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.
- viii. Un servicio de terminación de vigencia del Certificado.
- c. 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**.
- d. De los problemas surgidos durante notificación a la Autoridad Certificadora Raíz de la Secretaría de Economía, de una emisión o revocación de un certificado.
- e. Cumplir con el marco jurídico en lo referente a sus responsabilidades como Prestador de Servicios de Certificación, establecidos en el **REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación**, en las **REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación** y en el **Código de Comercio**.

### **2.3. Exclusión de responsabilidades PSC World como Agencia Certificadora**

- a. 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.
- b. De cualquier daño o perjuicio que se derive de utilizations 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.
- c. De la utilización del certificado para usos distintos de aquellos para los cuales se haya emitido.
- d. 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.
- e. 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 que ofrece.
- f. Del contenido de los documentos firmados digitalmente ni de las páginas Web que contengan un certificado por ella emitido.
- g. 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.

### **2.4. Obligaciones de PSC World como Agencia Registradora.**

- a. Registrar Certificados Digitales siempre y cuando se confirme la unicidad de las llaves públicas.
- b. Mantener un registro de certificados, en el que quedará constancia de los emitidos y figurarán las circunstancias que afecten a la suspensión o terminación de vigencia de sus efectos. Al contenido público de dicho registro estará disponible vía Web para las personas que lo soliciten, el contenido privado estará a disposición del Titular y/o de los usuarios que él autorice, así como en los casos a que se refieran las reglas generales que al efecto establezca la Secretaría.
- c. Administrar las bases de datos con los Certificados Digitales registrados, tanto actuales como históricas.
- d. Proteger los datos de carácter personal suministrados por el **Solicitante** de acuerdo a la **Política para el Manejo de Información Confidencial**.
- e. Ejecutar todas las actividades que le correspondan de acuerdo a la **Declaración de Prácticas de Certificación**.

### **2.5. Responsabilidades de PSC World como Agencia Registradora.**

- a. Conservar toda la información y documentación relativa a los certificados.
- b. Cumplir con el marco jurídico en lo referente a sus responsabilidades como Prestador de Servicios de Certificación, establecidos en el **REGLAMENTO del Código de Comercio en Materia de Prestadores de Servicios de Certificación**, en las **REGLAS generales a las que deberán sujetarse los prestadores de servicios de certificación** y en el **Código de Comercio**.

### **2.6. Exclusión de responsabilidades de PSC World como Agencia Registradora**

- a. 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.

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 6 de 12

- b. De 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 que ofrece.
- c. Tampoco será responsable frente a terceros afectados, que tengan una relación directa o indirecta con los servicios que presta la Agencia Registradora.
- d. 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.
- e. 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.
- f. 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.

**2.7. Obligaciones de los Agentes Certificadores**

- a. Solicitar a la Agencia Certificadora la emisión o revocación de certificados según sea el caso.
- b. Verificar la identidad de los **Solicitantes** y cualquier circunstancia pertinente para la emisión de los certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificado al **Solicitante**.
- c. Verificar y corroborar la información contenida en el **Requerimiento de Solicitud de Certificado Digital** con base en los documentos solicitados.
- d. Garantizar que el **Solicitante** cumpla con los requisitos establecidos en la **Declaración de Prácticas de Certificación**.
- e. Proteger los datos de carácter personal suministrados por el **Solicitante**.
- f. Ejecutar todas las actividades que le correspondan de acuerdo a la **Declaración de Prácticas de Certificación**.

**2.8. Responsabilidades de los Agentes Certificadores**

- a. Responder 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**.

**2.9. Exclusión de responsabilidades de los Agentes Certificadores.**

- a. 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.

**2.10. Obligaciones y responsabilidades 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**, presentando su **Requerimiento de Solicitud de Certificado Digital**.
- c. Conocer y aceptar las normas estipuladas en el **Acuerdo de Prestación de Servicios**.
- d. Ejecutar todas las actividades que le correspondan de acuerdo a la **Declaración de Prácticas de Certificación**.

**2.11. Responsabilidades de los Solicitantes y Titulares de certificados**

- a. Cumplir las obligaciones derivadas del uso de la Firma Electrónica, establecidas en el **“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 29-08-2003 o las modificaciones que actualicen la misma.
- b. Descargar su certificado digital ya registrado.
- c. Mantener en un lugar seguro su clave privada.
- d. No olvidar la frase de seguridad y mantenerla en secreto.
- e. Notificar a **PSC World** de cualquier modificación de sus antecedentes, que como consecuencia pudiera invalidar uno o más certificados emitidos a su nombre.
- e. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma Electrónica.
- f. 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.

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 7 de 12

**2.12. Responsabilidades de la Parte que Confía.**

- a. Evaluar, en forma independiente y libre, la procedencia y uso de un certificado en cualquier mensaje de datos y determinar si el certificado efectivamente podía ser utilizado para dicho propósito.
- b. Utilizar el software y/o hardware que resulten apropiados para desarrollar la verificación de la firma digital u otras operaciones criptográficas que deseen llevar a cabo, como condición para confiar en un certificado relacionado con cada una de dichas operaciones. Dichas operaciones incluyen la identificación de una cadena de certificación y la verificación de las Firmas Digitales incluidas en todos los certificados que forman parte de la cadena de certificación. La parte que Confía solamente podrá confiar en un certificado cuando dichos procedimientos de verificación acrediten su validez y vigencia.
- c. Verificar el estado de un certificado en el cual desea confiar, como así también el estado de todos los certificados en su cadena de certificación. Si cualquiera de los certificados de la cadena de certificación ha sido revocado, la Parte que Confía no podrá confiar en el certificado, ni en ninguno de los otros certificados revocados en la cadena de certificación.
- d. Confiar en el certificado solamente si todas las verificaciones descriptas anteriormente arrojan resultados satisfactorios y en la medida en que la confianza en dicho certificado resulte razonable. Si las circunstancias indican la necesidad de seguridades adicionales, es responsabilidad de la Parte que Confía, obtener las seguridades que estime razonable, para poder contar con dicha confianza.

**3. IDENTIFICACIÓN Y AUTENTICACIÓN****3.1. Método de verificación de identidad del solicitante**

- a. La verificación de la identidad del **Solicitante** se realizará por un **Agente Certificador**. El **Solicitante** tendrá que presentar original y copia para cotejo de los siguientes documentos en dependencia del tipo de certificado que se solicite:

**Certificado de Servidor**

Documentación a presentar ante Agente Certificador:

- Registro de dominio.
- Cédula del Registro Federal de Contribuyentes (Persona Moral) o Clave Única de Registro de Población (Persona Física).
- Identificación oficial (credencial para votar, pasaporte o cédula profesional).
- Comprobante de domicilio actual con una antigüedad no mayor a tres meses; tales como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.

**Certificado de Representación**

Documentación a presentar ante Agente Certificador:

**Persona moral:**

- Acta constitutiva.
- Escrituras de reformas a la constitutiva.
- Poder notarial del representante legal.
- Identificación oficial vigente del representante legal (credencial para votar, pasaporte o cédula profesional).
- Alta ante la Secretaría de Hacienda y Crédito público.
- Cédula del Registro Federal de Contribuyentes.
- Comprobante de domicilio actual con una antigüedad no mayor a tres meses; tales como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.

**Persona física:**

- Poder notarial del representante legal.
- Identificación oficial vigente del representante legal (credencial para votar, pasaporte o cédula profesional).
- Clave Única de Registro de Población o Cédula del Registro Federal de Contribuyentes.

- Comprobante de domicilio actual con una antigüedad no mayor a tres meses; tales como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.

### **Certificado Personal**

Documentación a presentar ante Agente Certificador:

- Identificación oficial vigente (credencial para votar, pasaporte o cédula profesional).
- Clave Única de Registro de Población.
- Comprobante de domicilio actual, con una antigüedad no mayor a tres meses; tales como recibo telefónico, luz o estados de cuenta de instituciones del sistema financiero, casas comerciales o tarjetas de crédito no bancarias.

- b. La verificación de la identidad de un Fedatario Público para la acreditación como **Agente Certificador**, se realizará por el Oficial de Seguridad de PSC World. El **Solicitante** tendrá que presentar original y copia para cotejo de los siguientes documentos en dependencia del tipo de certificado que se solicite:

#### **Notario Público**

- Identificación oficial vigente ( credencial para votar, pasaporte o cédula profesional)
- Clave Única de Registro de Población (CURP)
- Comprobante de domicilio actual con una antigüedad no mayor a tres meses; tal como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.
- Patente de Notario.

#### **Corredor Público**

- Identificación oficial vigente (credencial para votar, pasaporte o cédula profesional)
- Clave Única de Registro de Población (CURP)
- Comprobante de domicilio actual con una antigüedad no mayor a tres meses; tal como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.
- Habilitación para ejercer como Corredor Público.

- c. El **Agente Certificador** certificará la identidad del **Solicitante** corroborando la información contenida en el **Formato de Solicitud del Certificado** con base en los documentos solicitados.
- d. El **Agente Certificador** comprobará la razonable coincidencia entre la fotografía contenida en el documento de Identificación Oficial y la apariencia física del **Solicitante**.
- e. El **Agente Certificador** comprobará la razonable coincidencia entre la firma autógrafa contenida en el documento de Identificación Oficial y la registrada en el **Formato de Solicitud del Certificado**.
- f. Dicha presencia se registrará mediante la firma autógrafa en el **Convenio de Prestación de Servicios**.
- g. El **Agente Certificador** y la **Agencia Certificadora PSC World**, se reservan 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.
- h. El **Agente Certificador** y la **Agencia Certificadora 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.

### **3.2. Convenciones de nombre**

La **Agencia Certificadora PSC World** garantizará que su DN (Distinguished Names) sea único, asegurando la unicidad del mismo en cada certificado que emita.

#### **3.2.1. DN (Distinguished Names) de la Agencia Certificadora PSC World**

E = servicios@pscworld.com.mx

O = PSC World S.A. de C.V.

OU = PSC World

CN = Agencia Certificadora PSC World

STREET = Elena 359

PostalCode = 03500

C = MX

S = Distrito Federal

L = Nativitas

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 9 de 12

**3.2.2. DN (Distinguished Names) de los certificados emitidos por la Agencia Certificadora PSC World**

- E = <Correo electrónico>
- O = <Organización>
- CN = <Nombre del Titular>
- C = <País>

**3.3. Revocación de certificados****3.3.1. Periodo de validez de los certificados digitales**

- a. El periodo de validez del certificado digital de la **Agencia Certificadora PSC World** no será menor de 10 años y será emitido por la Agencia Certificadora Central de la Secretaria de Economía.
- b. Los certificados que emitirá la **Agencia Certificadora PSC World** a sus solicitantes de acreditación tendrán una validez de 1 año y será indicado en el certificado emitido.
- c. Los certificados caducarán automáticamente al finalizar dicho periodo, ocasionando la invalidez del certificado, el cese permanente de su operatividad y el término de la prestación de los servicios de certificación por **PSC World**.
- d. Al vencimiento del certificado podrá el Titular solicitar un nuevo certificado.

**3.3.2. Método de verificación del Titular**

- a. El **Titular** puede realizar la revocación vía Web a través del **Servicio de Certificación PSC World**, para lo cual requiere de la clave de anulación. Esto permite que solamente el usuario que conoce la clave de revocación de su propio certificado, lo pueda revocar.
- b. Si el **Titular** no tiene posibilidad de efectuar la revocación por el mecanismo anterior, deberá dirigirse personalmente ante un **Agente Certificador**, previamente habiendo completado y firmado el **Formato de Revocación de Certificado**. Para la acreditación de su identidad y/o personalidad deberá presentar una identificación oficial vigente (credencial para votar, pasaporte o cédula profesional).

**4. REQUERIMIENTOS OPERACIONALES****4.1. Procedimiento de Operación para Otorgar Certificados**

- a. Los procedimientos de operación para otorgar certificados digitales, queda descrito en la **Declaración de Prácticas de Certificación**.
- b. El proceso se puede describir en las siguientes subprocesos:
  - Proceso de solicitud del certificado: En este proceso el **Solicitante** realiza vía Internet su Requerimiento de Solicitud del Certificado y genera su par de llaves
  - Proceso de acreditación de la identidad y/o personalidad del **Solicitante**: En este proceso el **Solicitante** se presenta ante un **Agente Certificador** y acredita su identidad y/o personalidad.
  - Proceso de certificación de la identidad y/o personalidad del Solicitante: En este proceso el **Agente Certificador**, acredita la personalidad del Solicitante y procesa el Requerimiento de Solicitud de Certificado
  - Proceso de generación del certificado digital: En este proceso la **Agencia Certificadora PSC World** emite el Certificado Digital
  - Proceso de entrega del certificado: En este proceso el **Titular** descarga su certificado vía Web.
- c. **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.
- d. **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

**4.2. 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 la **Agencia Certificadora PSC World**
  - Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a un año, 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 **Titular** incumpla las condiciones de utilización de los certificados establecidas en el contrato con PSC World
- b. Condiciones para la revocación por la **Agencia Certificadora PSC World**, a solicitud del **Titular**, o por la persona física o moral representada por éste o por un tercero autorizado, o a través del **Servicio de Certificación PSC World** por el **Titular** 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,

#### 4.3. Distribución de certificados

- a. PSC World hará entrega del certificado a su **Titular** vía Web, notificándole de su disponibilidad por correo electrónico, una vez emitido por la **Agencia Certificadora PSC World**.
- b. El **Titular** de un certificado emitido por la **Agencia Certificadora PSC World**, podrá descargar su certificado a través del **Servicio de Certificación PSC World**.
- c. **PSC World** mantendrá en su sitio <http://www.pscworld.com> un repositorio con los certificados que ha emitido y revocado, mismo que estará disponible al público.

#### 4.4. Publicación de información de revocaciones

Para brindar un adecuado servicio de información sobre las revocaciones, **PSC World** soportará 3 medios para distribuir dicha información, las cuales se detallan a continuación:

1. **LISTAS DE REVOCACIÓN:** PSC World mantendrá la Lista de Certificados Revocados con la información de los certificados revocados o suspendidos,
2. **CHEQUEO DE REVOCACIÓN ON-LINE (OCSP):** PSC World soporta la consulta "on- line" sobre el estado de los certificados por ella emitidos, a través del protocolo OCSP (On- line Certificate Status Protocol).
3. **CONSULTA MEDIANTE EL WEB:** También se podrán consultar el estado de los certificados on- line mediante el uso del Web en <http://www.pscworld.com/pscworld>

#### 4.5. Frecuencia de actualización de la Lista de Certificados Revocados

La Lista de Certificados Revocados serán actualizadas con una frecuencia de 12 horas entre cada publicación.

#### 4.6. Auditoria

- a. **PSC World** manifiesta su conformidad para ser sujeto de auditoria por parte de la Secretaria de Economía en todo momento, para que ésta verifique el cumplimiento de los requisitos para obtener y mantener la acreditación como **Prestador de Servicios de Certificación**.
- b. **PSC World** tiene establecido un proceso de auditoria de seguridad de los servicios, que garantizan la continuidad del negocio.
- c. **PSC World** ha establecido un proceso de auditoria interna para garantizar el cumplimiento de los requisitos y mantener la acreditación como **Prestador de Servicios de Certificación** ante la Secretaria de Economía.
- d. **PSC World** será sujeto de un proceso de auditoria externa una vez al año, para garantizar el cumplimiento de los requisitos y mantener la acreditación como **Prestador de Servicios de Certificación** ante la Secretaria de Economía.

## 5. PRIVACIDAD Y SEGURIDAD

### 5.1. Requerimientos de Seguridad de la Agencia Certificadora PSC World

La **Agencia Certificadora PSC World** se encuentra instalada en **Prodigy Data Center** de **Telmex**

Ubicado en una zona de nula actividad sísmica, a sólo 5 minutos del Aeropuerto Internacional de la Ciudad de Monterrey, la **Agencia Certificadora PSC World** reside dentro de un bunker de concreto y acero armado protegido bajo otra estructura exterior de alta seguridad, con alambre de concertina y detectores de intrusos láser, más de 100 cámaras de vigilancia ubicadas en los exteriores e interiores del edificio, un sistemas de monitoreo continuo en sitio para controlar la seguridad física de las instalaciones, accesos restringidos a través de tarjetas de proximidad, sensores biométricos de huella y temperatura corporal, además puertas con esclusas de acero y vidrios anti-balas.

Los requerimientos de seguridad impuestos son:

- a. La Agencia Certificadora PSC World opera en un servidor de misión crítica redundante, protegido por múltiples sistemas de firewall, detectores de intrusos, sistemas de análisis de seguridad activos y sistemas de detección de incendios.
- b. Tanto el hardware como el software del servidor de misión crítica se encuentra en todo momento seguro.
- c. El intercambio de información Web con sus usuarios se realiza vía el protocolo SSL (Secure Socket Layer)
- d. La clave privada de la **Agencia Certificadora PSC World** se encuentra en todo momento cifrado en un dispositivo de alta seguridad FIPS 140-1 nivel 3.
- e. El par de claves RSA de la **Agencia Certificadora PSC World** tiene una longitud de 2048 bits.
- f. El par de claves RSA de los certificados emitidos por la **Agencia Certificadora PSC World** tendrá como mínimo una longitud de 1024 bits.
- g. Si la clave privada de la **Agencia Certificadora PSC World** se viera comprometida, se procedería a la revocación de la misma y del certificado, así como de todos los certificados emitidos por ella y no se emitirá certificado alguno hasta que se restaure la identidad de la **Agencia Certificadora PSC World**.

### 5.2. Requerimientos de Privacidad de la Agencia Certificadora PSC World

Para asegurar la privacidad de la información proporcionada por los clientes, **PSC World** ha establecido una **Política de Privacidad**, misma que se encuentra publicada en el sitio <http://www.pscworld.com/pscworld>

**PSC World** deja claramente establecido que no comparte, vende, cede, ni transfiere la información personal de los usuarios.

## 6. 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.

Documento: Política de Certificados		
Propietario: PSC World	Versión 2/022006	Número: POL002-PSCW
Clasificación de la Información: Pública		Página 12 de 12