

Declaración de Prácticas de Certificación PSC World

Tabla de Contenido

1. INTRODUCCIÓN	2
1.1. Sobre las Prácticas de Certificación	2
1.2. Alcance	2
1.3. Referencias	4
1.4. Definiciones	4
1.5. Comunidad y aplicabilidad	5
1.5.1. Comunidad de usuarios	5
1.5.2. Aplicabilidad de los certificados	5
1.5.3. Tipos y usos de los certificados	5
1.5.4. Precios de los certificados	7
1.5.5. Contenido de los Certificados	7
1.6. Contactos	7
2. OBLIGACIONES Y RESPONSABILIDADES	7
2.1. Obligaciones de PSC World como Agencia Certificadora	7
2.2. Responsabilidades de PSC World como Agencia Certificadora	8
2.3. Exclusión de responsabilidades PSC World como Agencia Certificadora	9
2.4. Obligaciones de PSC World como Agencia Registradora.	9
2.5. Responsabilidades de PSC World como Agencia Registradora.	9
2.6. Exclusión de responsabilidades de PSC World como Agencia Registradora	10
2.7. Obligaciones de los Agentes Certificadores	10
2.8. Responsabilidades de los Agentes Certificadores	10
2.9. Exclusión de responsabilidades de los Agentes Certificadores.	10
2.10. Obligaciones y responsabilidades de los Solicitantes y Titulares de certificados	10
2.11. Responsabilidades de los Solicitantes y Titulares de certificados	10
2.12. Responsabilidades de la Parte que Confía.	11
3. IDENTIFICACIÓN Y AUTENTICACIÓN	11
3.1. Método de verificación de identidad del solicitante	11
3.2. Convenciones de nombre	13
3.2.1. DN (Distinguished Names) de la Agencia Certificadora PSC World	13
3.2.2. DN (Distinguished Names) de los certificados emitidos por la Agencia Certificadora PSC World	13
3.3. Revocación de certificados	13
3.3.1. Periodo de validez de los certificados digitales	13
3.3.2. Método de verificación del Titular	13
4. PROCEDIMIENTO DE OPERACIÓN	14
4.1. El Solicitante	14
4.2. El Agente Certificador	15
4.3. La Agencia Certificadora PSC World	16
4.4. El Agente Certificador	16
4.5. El Titular	16
5. VIGENCIA DE LOS CERTIFICADOS Y PROCEDIMIENTOS DE REVOCACIÓN	16
5.1. Vigencia	16
5.2. Procedimientos para solicitar la revocación de un certificado	16
5.3. Procedimientos de publicación de información de revocaciones	17
6. INICIO DE OPERACIONES	17
7. PROTECCIÓN DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN.	17
8. PROCEDIMIENTO PARA REGISTRAR FECHA Y HORA DE TODAS LAS OPERACIONES RELACIONADAS CON LA EMISIÓN DE UN CERTIFICADO	19
9. PROCEDIMIENTO EN CASO DE SUSPENSIÓN TEMPORAL O DEFINITIVA DE PSC WORLD COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN	19
10. MEDIDAS DE SEGURIDAD ADOPTADAS PARA LA PROTECCIÓN DE LOS DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA	19
11. CONTROLES QUE SE UTILIZAN PARA ASEGURAR:	20
11.1. Que el propio usuario genere sus Datos de Creación de Firma Electrónica	20
11.2. Autenticación de Solicitantes	20
11.3. Autenticación de Agentes Certificadores Fedatario Público	20
11.4. Emisión de certificados	20
11.5. Revocación de certificados	21
11.6. Auditoría	21
11.7. Almacenamiento de información relevante	21

1. INTRODUCCIÓN

PSC World tiene como objetivo la implementación de los Servicios de Seguridad Administrados 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, institución pública o privada 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 estas prácticas de certificación..

1.1. Sobre las Prácticas de Certificación

En este documento se presentan las **Prácticas de Certificación** de PSC World. Estas son una descripción detallada de las normas o prácticas que **PSC World** declara convenir en la prestación de sus servicios de certificación, cuando emite y gestiona certificados digitales en su rol de Agencia Certificadora; además se incluyen las normas a seguir por la Agencia Registradora (AR) y los Agentes de Certificación acreditadas por **PSC World**.

Al emitir un certificado digital, una Agencia Certificadora establece cierto nivel de seguridad a todos los agentes que depositarán su confianza en la validez de dicho certificado, como instrumento que da garantías sobre la identidad del titular del mismo. En ese sentido, establece que se han tomado las medidas y procedimientos adecuados para constituir la correspondencia entre dicho certificado y una cierta entidad en particular (individuo, servidor, etc.).

Un mecanismo para evaluar la calidad y grado de confianza que se puede depositar en un certificado digital, es a través de la revisión de las prácticas usadas por la Agencia Certificadora para emitir dicho certificado, es decir, las **Prácticas de Certificación**.

Esta **Declaración de Prácticas de Certificación**, en conjunto con la **Política de Certificados**, 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.

Es una explicación detallada de las prácticas que **PSC World** emplea para emitir y gestionar certificados, y que implementa y soporta los requerimientos de las Políticas de Certificados.

Tales prácticas son las que se prosigue en detallar, y están disponibles en el sitio WEB de **PSC World** (<http://www.pscworld.com/pscworld>) para conocimiento público.

1.2. Alcance

Describir la Declaración de Prácticas de Certificación 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 (PKI) 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

En esta **Declaración de Prácticas de Certificación** 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.

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 2 de 21

- 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.

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.

Estos procedimientos se aplican a la Agencia Certificadora, Agencia Registradora, Agentes Certificadores, Solicitantes y Titulares, para la emisión de Certificados por **PSC World**, de acuerdo con cada tipo de certificado y las limitaciones de uso establecidas para cada caso.

Forma parte de esta **Declaración de Prácticas de Certificación**, un conjunto de documentos que por su carácter de información pueden o no estar publicadas, entre los que se encuentran:

Documento	Descripción	Carácter
Modelo Operacional	El modelo operacional define cómo PSC World prestará sus servicios al fungir como Agencia Certificadora y Agencia Registradora, a efecto de lograr confiabilidad e interoperatividad con sus Solicitantes de Acreditación	Confidencial
Plan de Seguridad de Sistemas	Tiene como objetivo definir e implantar estrategias de mitigación de riesgos en la infraestructura requerida para la operación del negocio.	Confidencial
Plan de Administración de Claves	El Plan de Administración de claves tiene como objetivo definir e implantar el plan de administración del ciclo de vida de las llaves, permitiendo proteger y administrar las llaves criptográficas y garantizar su seguridad en todo momento, aun en caso de cambios de personal o componentes tecnológicos	Confidencial
Plan de Continuidad del Negocio y Recuperación ante Desastre	Estable cómo PSC World reaccionará ante la interrupción de actividades del negocio y protegerá sus procesos críticos frente a grandes fallos o desastres.	Confidencial
Política de Privacidad	Establece el tratamiento que PSC World dará a la información recopilada, almacenada y transmitida durante la prestación de sus servicios	Pública
Política para el Manejo de Información Confidencial	Su objetivo es asegurar que la información confidencial generada, almacenada y transmitida no ha sido modificada, azezada o extraída por personal no autorizado de manera intencionada y/o accidental.	Confidencial
Política de Seguridad de la Información	El objetivo de esta política es proteger los activos de información de la Empresa de amenazas internas o externas, deliberadas o accidentales.	Confidencial
Política de Seguridad Física	Tiene como objetivo asegurar que el ingreso a las instalaciones de PSC World, se realice en forma controlada, autorizada y justificada, reduciendo las posibilidades de que alguna persona pueda introducirse a la instalación y provocar alguna afectación premeditada y/o accidental, que ponga en riesgo los servicios proporcionados por la empresa.	Confidencial
Política de Control de Cambios	Asegura que cualquier modificación a la infraestructura tecnológica de PSC World se realice sin impacto a los servicios	Confidencial
Procedimiento para la Gestión Interna de Soporte	Asegura la atención oportuna que cualquier incidencia en los servicios con el objetivo de minimizar su impacto.	Confidencial
Manual de solicitud del certificado	Es una guía para la solicitud de los certificados	Pública
Manual de Procedimientos de Instalación de la Agencia Certificadora	Es un manual orientado al personal que instalará la Autoridad Certificadora y Registradora.	Confidencial
Manual de Procedimientos de la Agencia Certificadora y Registradora	Es un manual orientado al personal que operará la Autoridad Certificadora y Registradora a través de la consola de Administración	Confidencial
Manual de Procedimientos del Agente	Es un manual orientado a los Agentes Certificadores acreditados	Confidencial

Documento: Declaración de Prácticas de Certificación

Propietario: PSC World S.A. de C.V.

Versión 2/022006

Número: OPE001-PSCW

Clasificación de la información: Pública

Página 3 de 21

Certificador	por PSC World	
Manual de Procedimientos para la Instalación SeguriSuite	Especifica los aspectos técnicos y operativos necesarios con que se deben contar para realizar de manera adecuada la implementación de los productos que soportan la operación de la Autoridad Certificadora y Registradora.	Confidencial
Manual de Procedimientos RRHH	Establece las políticas y procedimientos para la contratación del personal que laborará en PSC World	Confidencial
Acuerdo de Prestación de Servicios	Es el acuerdo que se establece entre PSC World y el TITULAR del Certificado para la prestación de los servicios en materia de firma electrónica y expedición de certificados digitales	Pública
Contrato Agente Certificador	Es el convenio para la prestación de los servicios de certificación en materia de firma electrónica y expedición de certificados digitales que celebra PSC World para acreditar sus Agentes Certificadores.	Confidencial
Convenio de Confidencialidad AGENTE	Es el convenio de confidencialidad para el manejo de la información que celebra PSC World con los Agentes Certificadores acreditados	Confidencial
Convenio de Confidencialidad EMPLEADOS.	Es el convenio de confidencialidad para el manejo de la información que celebra PSC World con sus empleados.	Confidencial
Formato de Solicitud del Certificado	Es el formato establecido para la solicitud de un certificado digital	Pública
Formato de Revocación del Certificado	Es el formato establecido para la solicitar la revocación de un certificado digital ante un Agente Certificador.	Pública

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.

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.

<i>Documento: Declaración de Prácticas de Certificación</i>		
<i>Propietario: PSC World S.A. de C.V.</i>	<i>Versión 2/022006</i>	<i>Número: OPE001-PSCW</i>
<i>Clasificación de la información: Pública</i>		<i>Página 4 de 21</i>

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 y aplicabilidad

1.5.1. Comunidad de usuarios

PSC World emite Certificados Digitales basados en la estándar ITU-T Recommendation X.509.

Todos los certificado emitidos por **PSC World** son emitidos a personas físicas y organizaciones públicas o privadas. En el primer caso, 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. Aplicabilidad de los certificados

Los Certificados emitidos por la **Agencia Certificadora PSC World**, no han sido diseñados, orientados ni se autoriza su utilización o reventa para controlar equipos en situaciones peligrosas o para su empleo en aplicaciones que requieran la ausencia total de fallas, tal como la operación de instalaciones nucleares, sistemas de navegación o comunicación de aeronaves, sistemas de control de tráfico aéreo o sistemas de control de armamento, en donde una falla puede derivar en muerte, lesiones a personas o daños serios al medio ambiente, siendo esta enumeración meramente ejemplificativa y no limitativa de supuestos de improcedencia de uso.

Los certificados de **PSC World** podrán ser aplicados para soportar las siguientes necesidades de seguridad:

Autenticación: proporciona suficientes garantías respecto a la identidad del Titular del certificado, al requerirse su presencia física ante un Agente certificador, junto con los documentos establecidos en el **Formato de Solicitud del Certificado**, que acreditan su identidad y/o personalidad.

Integridad: los mensajes firmados con los certificados de **PSC World**, permiten validar si el contenido de un mensaje de datos ha sido alterado en el tiempo transcurrido entre su envío y su recepción efectiva.

No repudiación: las firmas digitales producidas con los certificados de **PSC World**, 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: los certificados de **PSC World**, permiten cifrar mensajes de forma que al ser transmitidos o almacenados, solo sean observados por el Titular de los Datos de Creación de Firma Electrónica.

1.5.3. Tipos y usos de los certificados

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

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 5 de 21

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 Sockets Layer).

Secure Sockets Layer, es un protocolo diseñado por Netscape Communications para habilitar las comunicaciones de manera encriptada y autenticada a través del Internet; es usado principalmente (aunque no de manera exclusiva) en comunicaciones entre Navegadores y Servidores Web, proporcionando tres factores de seguridad importantes:

Privacidad: Se encripta todo lo que se envía en cada extremo, asegurando que sólo el destinatario deseado pueda descifrarlo.

Autenticación: El extremo receptor puede asegurarse que los datos provienen del lugar a dónde se están solicitando.

Integridad en los Mensajes: Se asegura que el mensaje no ha sido alterado o manipulado por ajenos.

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 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**.

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

		<ul style="list-style-type: none">▪ Firma de documentos▪ Firma de contratos
Todos los Certificados emitidos por PSC World tienen el mismo nivel de Seguridad.		

1.5.4. Precios de los certificados

Los precios para la emisión de los certificados están determinados por tres factores:

1. Tipo de certificado.
2. Tipo de certificación :
 - **Con Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante.
 - **Sin Fe Pública** de acreditación de la identidad y/o personalidad del Solicitante.
3. Condiciones comerciales.

Características de la certificación "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).

Características de la certificación "Sin Fe Pública": Son acreditados ante un Agente Certificador de PSC World.

La lista de precios actualizada estará disponible en el sitio Web <http://www.pscworld.com/pscworld>

1.5.5. Contenido de los Certificados

La estructura de datos del Certificado emitido por PSC World es compatible con el estándar ISO/IEC 9594-8 y su contenido cumple con el artículo 108 de Código de Comercio.

Los certificados emitidos por PSC World contendrán:

- Indicación de expedición
- Código de identificación único del Certificado
- Identificación de PSC World
 - Razón Social: PSC World S.A. de C.V
 - Domicilio: México D.F.
 - Dirección de correo electrónico: servicios@pscworld.com.mx
 - Datos de acreditación ante la Secretaría
- Nombre del titular del certificado
- Periodo de vigencia del certificado
- Fecha y hora de emisión
- Alcance de las responsabilidades que asume PSC World
- Referencia de la tecnología empleada para la generación de la firma electrónica
- Referencia para localizar un sitio de consulta donde se publiquen las notificaciones de revocación de los certificados o los que la Secretaría especifique.

1.6. Contactos

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

e-mail: 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.

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 7 de 21

- b. Mantener en todo momento protegido sus datos de Creación de Firma Electrónica, mismos que se encuentran resguardados en una tarjeta CryptoSwift HSM de Rainbow, certificada en el estándar FIPS 140-1 nivel 3
- 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.
- h. 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.
- i. Publicar los certificados emitidos en su sitio Web para consulta de cualquier usuario.
- j. Permitir la consulta en línea de su certificado.
- k. 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.
- l. 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**
- m. 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.
- n. 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.
- o. No emitir certificados con una duración superior a la vigencia de su vínculo administrativo con el solicitante.
- p. Contar con los elementos humanos, materiales, económicos y tecnológicos que garanticen la seguridad y operación de los servicios.
- q. Establecer declaraciones sobre sus normas y prácticas, las cuales harán del conocimiento del usuario y el destinatario.
- r. Proteger los datos de carácter personal suministrados por el Solicitante de acuerdo a la **Política para el Manejo de Información Confidencial**.
- s. 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: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 8 de 21

- 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.
- viii. Si se ofrece 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 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 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**

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 9 de 21

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.
- 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. 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.

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 de acuerdo a la **Política para el Manejo de Información Confidencial**.
- 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

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 10 de 21

“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.

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. La validación se puede realizar consultando en el sitio Web de **PSC World** la Lista de Certificados Revocados (CRL), o el estado del Certificado en la Consulta de Certificados Digitales.
- 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

1. 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.

<i>Documento: Declaración de Prácticas de Certificación</i>		
<i>Propietario: PSC World S.A. de C.V.</i>	<i>Versión 2/022006</i>	<i>Número: OPE001-PSCW</i>
<i>Clasificación de la información: Pública</i>		<i>Página 11 de 21</i>

- 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.

2. 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, quien fungirá para ese acto como **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:

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.

3. 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.
4. El Agente Certificador comprobará la razonable coincidencia entre la fotografía contenida en el documento de Identificación Oficial y la apariencia física del Solicitante.
5. 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.

6. Dicha presencia se registrará mediante la firma autógrafa en el **Convenio de Prestación de Servicios**.
7. 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.
8. 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

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

E = <Correo electrónico>
O = <Registro Federal de Contribuyentes>
CN = <Nombre del Titular>
C = MX

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 Secretaría 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, que será emitido a un menor costo.

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. Allí deberá estampar su firma autógrafa en una solicitud de revocación, en la que se establece el momento en que se solicita la misma junto con sus datos. Para la acreditación de su identidad y/o personalidad deberá presentar una identificación oficial vigente (credencial para votar, pasaporte o cédula profesional).

4. PROCEDIMIENTO DE OPERACIÓN**4.1. El Solicitante**

Para que el **Solicitante** pueda realizar el proceso de registro y obtener su certificado digital, tendrá la obligación de:

- I. Consultar el **Manual de Usuario** en la ruta <http://www.pscworld.com/pscworld>. Este manual describe de manera detallada los pasos a seguir para la generación de las llaves y del certificado.
- II. Descargar y completar el **Formato de Solicitud del Certificado**. Este documento es una forma que debe ser completado y firmado por el **Solicitante**, anexando al mismo los documentos a presentar ante el **Agente Certificador** para acreditar su personalidad o identidad.
 - a. Descargar el **Formato de Solicitud del Certificado** en la ruta <http://www.pscworld.com/pscworld>
 - b. Imprimir **Formato de Solicitud del Certificado**.
 - c. Completar **Formato de Solicitud del Certificado**.
- III. **Solicitar Certificado** en la ruta <http://www.pscworld.com/pscworld>. En este proceso el **Solicitante** genera su par de llaves (pública y privada) a través del **Servicio de Certificación PSC World**. Los requerimientos mínimos son:
 - Computadora personal con sistema operativo Windows 98 / 2000 / ME / XP (con todos los parches y actualizaciones instalados).
 - Microsoft Internet Explorer 5.5 o superior (con todos los parches instalados).
 - Conexión a Internet.La llave privada se mantiene localmente en el equipo de cómputo del Solicitante en el repositorio de llaves de su Cryptographic Service Provider, mientras que la llave pública es enviada a la **Agencia Certificadora PSC World** como **Requerimiento de Certificación** (archivo PKCS 10). Para realizar este proceso se requiere completar los siguientes pasos:
 - a. Acceder a la opción **Solicitud del Certificado** del menú **Servicios de Certificación PSC World**.
 - b. Llenar la forma con los datos solicitados, necesarios para crear el par de llaves.
 - c. Seleccionar el nivel de seguridad; mismo que se tiene que establecer como **Alto** (High).
 - d. Generar las llaves.
- IV. Imprimir el **ID del Requerimiento** que se obtiene al terminar el proceso de **Solicitud del Certificado** para su presentación ante el **Agente Certificador**.
- V. Presentar documentación de acreditación de la personalidad o identidad ante un **Agente Certificador** autorizado por **PSC World**.
 - a. Podrá acceder a la lista de los Agentes Certificadores autorizados por **PSC World** en la ruta <http://www.pscworld.com/pscworld>
 - b. Presentar original y copia para cotejo de los siguientes documentos:
 - Persona Física**
 - 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 recibo telefónico, luz o estados de cuenta de instituciones del sistema financiero, casas comerciales o tarjetas de crédito no bancarias.
 - Formato de Solicitud del Certificado.
 - ID del Requerimiento.
 - 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).
 - Registro Federal de Contribuyentes.
 - 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; tal como boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.
- Formato de Solicitud del Certificado.
- ID del Requerimiento.

Fedatario Público para Contrato de Agente Certificador

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.
- Formato de Solicitud del Certificado.
- ID del Requerimiento.

Corredor Público

- Identificación oficial vigente; credencial para votar, pasaporte o cédula profesional.
- 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.
- Formato de Solicitud del Certificado.
- ID del Requerimiento.

4.2. El Agente Certificador

VI. Certifica la identidad del Solicitante.

- a. Corrobora la semejanza entre los rasgos físicos del **Solicitante** y el documento de identificación oficial.
- b. Corrobora la semejanza entre la firma autógrafa del **Solicitante** y el documento de identificación oficial.

VII. Verifica y corrobora la información contenida en el **Formato de Solicitud del Certificado** con base en los documentos solicitados.

- a. De existir alguna discrepancia entre la documentación solicitada para cotejo y la información registrada el **Formato de Solicitud del Certificado**, la solicitud será rechazada.
- b. El **Agente Certificador** se reserva el derecho a solicitar cualquier información adicional al **Solicitante** o a terceros, que permita la verificación de la documentación.

VIII. Procesa el **Requerimiento de Certificación**.

- a. En este proceso el **Agente Certificador** firma digitalmente el **Requerimiento de Certificación** del **Solicitante**, generando un **Precertificado** que se transmite a la **Agencia Certificadora PSC World**. Para realizar este proceso se requiere completar los siguientes pasos:
 1. Entrar a la aplicación SeguriServer Agente y recuperar el **Requerimiento de Certificación** del **Solicitante** (archivo PKCS 10) por medio del campo *ID del Requerimiento*.
 2. Valida y corrobora la documentación solicitada para cotejo contenida en el **Formato de Solicitud del Certificado** con la registrada en el **Requerimiento de Certificación**, con base en los documentos solicitados; de existir alguna discrepancia, se cancela el proceso y la solicitud será rechazada.
 3. Seleccionar las características del **Certificado** que será generado.

4. Realiza certificación del requerimiento, firmando digitalmente el **Requerimiento de Certificación** del **Solicitante**, generando un **Precertificado**, mismo que es enviado a la **Agencia Certificadora PSC World**.
- IX. El **Agente Certificador** se reserva el derecho a no procesar el **Requerimiento de Certificación** cuando así lo estime conveniente, comunicando las razones de la negación, sin que por ello pueda exigirse responsabilidad alguna.
- 4.3. La Agencia Certificadora PSC World**
- X. Recibe el **Precertificado** y valida la firma electrónica del **Agente Certificador**.
- XI. Emite el Certificado Digital del **Solicitante** con su firma electrónica.
- XII. Envía el certificado a la **Agencia Registradora** para su registro.
- XIII. Envía **Recibo de Emisión del Certificado** al **Agente Certificador**.
- XIV. Envía correo electrónico al **Solicitante** con ruta de descarga de su Certificado.
- XV. 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
- 4.4. El Agente Certificador**
- XVI. Imprime para firma del **Titular**, el **Recibo de Emisión del Certificado** y el **Acuerdo de Prestación de Servicios**.
- XVII. Crea expediente del **Titular** resguardando copia de:
- Formato de Solicitud del Certificado.
 - ID del Requerimiento.
 - Documentación de acreditación de la personalidad o identidad del **Solicitante**.
 - Recibo de Emisión del Certificado firmado por el **Titular**.
 - Acuerdo de Prestación de Servicios firmado por el **Titular**.
- 4.5. El Titular**
- XVIII. Firma **Recibo de Emisión del Certificado** y **Acuerdo de Prestación de Servicios**
- XIX. Descargar certificado por medio del:
- Servicio de Certificación PSC World** en la ruta <http://www.pscworld.com/pscworld>
 - Ruta especificada en el correo enviado por la **Agencia Certificadora PSC World**.

5. VIGENCIA DE LOS CERTIFICADOS Y PROCEDIMIENTOS DE REVOCACIÓN

5.1. Vigencia

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

- 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. Antes de que concluya el periodo de vigencia del Certificado podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación.
- Revocación por el Prestador de Servicios de Certificación, a solicitud del **Titular**, o por la persona física o moral representada por éste o por un tercero autorizado.
- Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado.
- 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 la seguridad de la clave privada se haya comprometido.
- 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**.

5.2. Procedimientos para solicitar la revocación de un certificado

- I. El Titular puede realizar la revocación a través del **Servicio de Certificación PSC World**, en la ruta <http://www.pscworld.com/pscworld>

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 16 de 21

- II. Si el Titular no tiene posibilidad de efectuar la revocación por el mecanismo anterior, deberá dirigirse personalmente ante un **Agente Certificador**. Allí deberá estampar su firma holográfica en una solicitud de revocación, en la que se establece el momento en que se solicita la revocación junto con sus datos.
- III. Una vez recibida la solicitud de revocación en **PSC World** esta es procesada generándose inmediatamente la revocación efectiva del certificado correspondiente.

5.3. Procedimientos de publicación de información de revocaciones

- I. 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:
 - a. **LISTAS DE REVOCACIÓN:** PSC World mantendrá la Lista de Certificados Revocados con la información de los certificados revocados o suspendidos. Estas listas están en un formato compatible con el estándar ISO/IEC 9594-8 y en cada certificado emitido, en la extensión apropiada, se incluirá la información de la ubicación de la lista de revocación para su consulta.
 - b. **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).
 - c. **CONSULTA MEDIANTE EL WEB:** También se podrán consultar el estado de los certificados en el sitio Web de PSC World <http://www.pscworld.com/pscworld>
- II. La información respecto a la revocación de un certificado quedará disponible en el sitio Web inmediatamente después de completado el proceso de revocación.
- III. La Lista de Certificados Revocados será actualizada con una frecuencia de 12 horas entre cada publicación.

6. INICIO DE OPERACIONES

El 15 de Diciembre de 2005 se publica en el Diario Oficial de la Federación la resolución por la que se otorga la acreditación como Prestador de Servicios de Certificación a PSC World, S.A. de C.V.

PSC World, S.A. de C.V., inicia sus operaciones el 16 de Diciembre de 2005

7. PROTECCIÓN DE CONFIDENCIALIDAD Y SEGURIDAD DE LA INFORMACIÓN.

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

PSC Word se rige por su **Política de Privacidad** para la protección de la confidencialidad de la información.

Para proteger la información de sus clientes, **PSC World** ha establecido además un conjunto de políticas y procedimientos de seguridad de acceso a la información denominado **“Política para el Manejo de Información Confidencial”**

PSC World para la prestación de sus servicios, integra a sus políticas y procedimientos los servicios de seguridad que brinda **Prodigy Data Center** (<http://triar.com>)

Prodigy Data Center es un centro de datos de clase mundial con el máximo nivel de seguridad para resguardar el equipo y la información de los clientes de **PSC World**, incorporando múltiples medidas para su protección, combinando varios mecanismos restrictivos y procesos para aumentar al máximo la seguridad.

Ubicado en una zona de nula actividad sísmica, a sólo 5 minutos del Aeropuerto Internacional de la Ciudad de Monterrey, **Prodigy Data Center de Telmex** es una formidable instalación que reside dentro de un bunker de concreto y acero armado protegido bajo otra estructura exterior de alta seguridad.

En **Prodigy Data Center**, las áreas y los servicios en los cuales se manejan información confidencial cuentan con procedimientos de control de acceso, supervisados continuamente a efecto de reducir al mínimo los riesgos, estos procedimientos se describen en la **“Política de**

Documento: Declaración de Prácticas de Certificación		
Propietario: PSC World S.A. de C.V.	Versión 2/022006	Número: OPE001-PSCW
Clasificación de la información: Pública		Página 17 de 21

Seguridad Física de PSC World". Los controles implementados evitan riesgos, daño o pérdida de los activos, alteración o sustracción de la información.

Mientras que los servicios compartidos por otra entidad distinta a **PSC World**, o por personal de éste no dedicado al servicio de certificación, se encuentra fuera del perímetro de seguridad.

7.1. Seguridad Física

- I. Un solo punto de acceso al Centro de Datos, protegido por personal de seguridad las 24 horas del día.
- II. Acceso a visitantes con escolta y sólo con cita previa autorizada del Oficial de Seguridad de PSC World.
- III. Muro perimetral con alambre de concertina y detectores de intrusos láser.
- IV. Más de 100 cámaras de vigilancia ubicadas en los exteriores e interiores del Edificio.
- V. Sistemas de monitoreo continuo en sitio para controlar la seguridad física de las instalaciones.
- VI. Acceso restringido al Centro de Datos a través de tarjetas de proximidad, sensores biométricos de huella y temperatura corporal, vidrios anti-balas nivel 7 y puertas con esclusas de acero.

7.2. Seguridad Lógica

- I. Múltiple tecnología de firewall
- II. Sistema de detección de intrusos
- III. Sistemas de análisis de seguridad activos

7.3. Sistema de Energía Eléctrica

Prodigy Data Center cuenta con un avanzado esquema de redundancia de suministro de energía que supera los estándares tradicionales de los Centros de Datos en el mundo.

Prodigy Data Center recibe energía eléctrica del exterior, de 2 subestaciones de generación de la Comisión Federal de Electricidad (CFE) independientes entre sí, con el propósito de obtener suministro redundante.

En el remoto caso de un corte de las dos líneas de la CFE, tiene implementado un sistema de respaldo que consiste en 6,000 baterías y 24 UPS de 500 Kva, reforzados por 18 generadores de energía, con una potencia total de salida de 30,000,000 de Watts, que son alimentados por múltiples tanques de diesel.

7.4. Sistema de Control Ambiental

El sistema ambiental de **Prodigy Data Center** funciona a través de un control automatizado que regula tanto la temperatura como las condiciones de humedad del Centro a través de 96 unidades de aire acondicionado de precisión con una capacidad de 30 toneladas cada una.

La distribución del aire brinda circulación ininterrumpida bajo el piso falso anti-estático, y le ofrece flujo preferente a los racks para prolongar el periodo de vida útil de los equipos. **Prodigy Data Center** utiliza también aires de precisión en los componentes críticos de la infraestructura de energía eléctrica.

7.5. Sistema de Extinción y Control de Incendios

Como primera línea de defensa ante un incendio, el **Prodigy Data Center** ha incorporado un sistema de detección de incendios capaz de identificar sensibles incrementos en la temperatura del cableado y otros componentes críticos de la infraestructura del Centro de Datos. De esta manera, el personal puede tomar acciones preventivas para eliminar un posible foco de siniestro.

No obstante, en el lejano caso de un siniestro, el **Prodigy Data Center** cuenta con un eficiente sistema de extinción vía gas Inergen, ya que no crea neblina al ser expulsado, para no disminuir la visibilidad de las salidas de emergencia y no deja residuos que afecten los equipos de cómputo.

7.6. Telecomunicaciones

Prodigy Data Center cuenta con enlaces a Internet de alta velocidad a más de 300 Mbps, conectados directamente al backbone nacional e internacional de Internet, con capacidad ya

<i>Documento: Declaración de Prácticas de Certificación</i>		
<i>Propietario: PSC World S.A. de C.V.</i>	<i>Versión 2/022006</i>	<i>Número: OPE001-PSCW</i>
<i>Clasificación de la información: Pública</i>		<i>Página 18 de 21</i>

construida en sitio para un crecimiento a más de 4.90 Gbps, manteniendo redundancia gracias a 2 anillos de fibra óptica redundantes.

8. PROCEDIMIENTO PARA REGISTRAR FECHA Y HORA DE TODAS LAS OPERACIONES RELACIONADAS CON LA EMISIÓN DE UN CERTIFICADO

- I. Las fechas manejadas por los productos de **PSC World** son UTC, esta se basa en un inicio en el reloj del equipo en el que están instaladas. Todas las transacciones de los productos llevan consigo un recibo en el cual se contiene la fecha y hora de emisión. Esta se complementa con una conexión a una fuente confiable de tiempo donde se emiten Estampado de Tiempo en base a un reloj atómico.
- II. **PSC World** llevará además un registro del Sistema de Sello o Estampado de Tiempo que se sincronizará con el de la Secretaría, para asegurar la fecha y la hora de la emisión de los certificados generados.
- III. El Sistema de Sello o Estampado de Tiempo utilizado por **PSC World** está basado en el estándar internacional Internet X.509 Public Key Infrastructure Time Stamp y considerar el RFC 3161.
- IV. **PSC World** asegurará en todo momento el enlace del Sistema de Sello o Estampado de Tiempo con el de la **Secretaría**.

9. PROCEDIMIENTO EN CASO DE SUSPENSIÓN TEMPORAL O DEFINITIVA DE PSC WORLD COMO PRESTADOR DE SERVICIOS DE CERTIFICACIÓN

- I. **PSC World** se compromete al cumplimiento de los procedimientos que establezca la **Secretaría**.
- II. **PSC World** se compromete al envío en línea de cada Certificado a la **Secretaría**, lo cual será en tiempo real.
- III. **PSC World** se compromete que en caso fortuito o de fuerza mayor de que no pudiese llevar a cabo el envío a que se refiere el apartado anterior realizará la réplica por cualquier medio en un término no mayor a seis horas.
- IV. Además del envío en línea de la copia de los Certificados, **PSC World** remitirá dicha copia a la **Secretaría** en medios ópticos o electrónicos dentro de las veinticuatro horas siguientes a la generación de los Certificados, a fin de garantizar redundancia del procedimiento técnico.
- V. **PSC World** se compromete a cerciorarse que la **Secretaría** ha recibido la copia de cada certificado por ella emitido.
- VI. En caso de suspensión definitiva o temporal **PSC World** entregará en medio óptico o electrónico, respaldo de la base de datos de los certificados a la **Secretaría** o Prestador de Servicios de Certificación por esté designado. Dicho acto de respaldo y entrega será protocolizado ante notario público.
- VII. El procedimiento de respaldo se realizará de acuerdo al Anexo A3 “Respaldos y Restauración” del Contrato TRIARA.
- VIII. **PSC World** en caso de suspensión temporal desactivará la tarjeta CrypSwift HSM desconectando el Token USB Trusted Channel de Operación, mismo que será entregado a la **Secretaría** hasta reactivar sus operaciones o se cambie el estatus de la suspensión a definitiva.
- IX. **PSC World** en caso de suspensión definitiva borrará la clave utilizada para los Datos de Creación de Firma Electrónica.y extraerá del equipo en el cual se encuentre instalado la tarjeta CrypSwift HSM.

10. MEDIDAS DE SEGURIDAD ADOPTADAS PARA LA PROTECCIÓN DE LOS DATOS DE CREACIÓN DE FIRMA ELECTRÓNICA

- I. Durante todo el proceso de **Generación del Requerimiento de Certificación** el Solicitante se encontrará en un sitio seguro del servicio Web de **PSC World**, protegido por el protocolo SSL (Secure Socket Layer).
- II. El procedimiento utilizado por **PSC World** para la generación de un Certificado Digital, se

basa en el hecho de recibir un Requerimiento de Certificación vía Web, por lo que la seguridad para la protección de los Datos de Creación de Firma Electrónica la brinda los Cryptographic Service Provider que utiliza el Navegador Web del Solicitante.

- III. **PSC World** generará sus Datos de Creación de Firma Electrónica, en el nivel de seguridad más alto de sus instalaciones, a fin de dar certeza y seguridad a todos los elementos necesarios para la creación de los mismos y bajo la supervisión de la **Secretaría**.

11. CONTROLES QUE SE UTILIZAN PARA ASEGURAR:

11.1. **Que el propio usuario genere sus Datos de Creación de Firma Electrónica**

Los **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.

Esta se genera por el solicitante durante el proceso de **Solicitud del Certificado** a través del **Servicio de Certificación de PSC World**

Para garantizar que el propio usuario genere sus **Datos de Creación de Firma Electrónica** la solución implementada por **PSC World** genera el par de claves (públicas y privadas) en el Navegador Web del Solicitante utilizando la protección de sus Cryptographic Service Provider, quedando la clave privada almacenada en el repositorio de claves del Sistema Operativo o del dispositivo determinado por el Cryptographic Service Provider.

Es importante especificar que el solicitante tiene la responsabilidad de la custodia de los **Datos de Creación de Firma Electrónica** asociados a su certificado.

11.2. **Autenticación de Solicitantes**

La autenticación de los **Solicitantes** de PSC World que tramitan un certificado se realiza a través de los **Agentes Certificadores** acreditados por **PSC World**.

PSC World acredita dos tipos de **Agentes Certificadores**, denominados:

- **Agentes Certificadores Fedatarios Públicos:** Son Notarios o Corredores Públicos acreditados por **PSC World** y que emiten certificados otorgando fe pública de la identidad o personalidad del **Solicitante**.
- **Agentes Certificadores PSC World:** Son personas físicas o morales acreditados por PSC World que emiten certificados sin fe pública de la identidad o personalidad del Solicitante.

Para garantizar la autenticación de los usuarios, el **Agente Certificador** está obligado a cumplir con el procedimiento descrito en el apéndice 4 **“PROCEDIMIENTO DE OPERACIÓN”** de este documento, cotejando la firma autógrafa y fisonomía del solicitante con los documentos solicitados.

11.3. **Autenticación de Agentes Certificadores Fedatario Público**

La autenticación de los Fedatarios Públicos para su registro como **Agentes Certificadores**, se realizará por el Oficial de Seguridad de PSC World S.A de C.V.

El procedimiento para la emisión del certificado de los **Agentes Certificadores Fedatario Público** por la **Agencia Certificadora PSC World**, es el mismo que se describe en el apartado 4 **“PROCEDIMIENTO DE OPERACIÓN”** de este documento, cotejando el Oficial de Seguridad de PSC World, la firma autógrafa y fisonomía del solicitante con los documentos solicitados.

11.4. **Emisión de certificados**

Para garantizar la emisión de los certificados, **PSC World** cuenta con una infraestructura redundante en alta disponibilidad en todos los componentes de su cadena de servicios que asegura la continuidad del negocio. Los controles incluyen un monitoreo constante de

todos los indicadores críticos de su infraestructura y un centro de atención y soporte a sus clientes

11.5. Revocación de certificados

Para garantizar la revocación de los certificados PSC World ha implementados varios mecanismos y controles que permiten lograr este objetivo; mismos que se describen en el apéndice 7.2 *“Procedimientos para solicitar la revocación de un certificado”* de este documento.

El constante monitoreo de los niveles de servicio de la infraestructura tecnológica de **PSC World**, es un control que garantiza a nuestros clientes la disponibilidad del servicio de revocación de los certificados; además de contar con el centro de atención y soporte que podría en caso necesario realizar esta actividad.

11.6. Auditoría

Para garantizar una constante auditoria de los servicios que ofrece **PSC World**, nuestra empresa ha habilitado un conjunto de registro de eventos en sus diferentes activos y un sistema de respaldo de los mismos que permiten su análisis posterior.

El módulo de auditoria de **SeguriServer** permite verificar la integridad de la base de datos, además de emitir reportes sobre las actividades de la **Agencia Certificadora**. Los procedimientos permiten:

1. Autenticar los registros de las bases de datos.
2. Generar reportes de actividad.

11.7. Almacenamiento de información relevante

Para garantizar el almacenamiento de información relevante PSC World cuenta con una infraestructura redundante y en alta disponibilidad de sus bases de datos

Los controles de respaldo y recuperación garantizan la disponibilidad de la información almacenada en caso de contingencia y el constante monitoreo de los umbrales de las bases de datos, es un control que garantiza a nuestros clientes la disponibilidad del servicio

Los controles de seguridad aunada a la política de seguridad, garantiza que solo el personal autorizado tenga acceso a la información relevante, evitando una modificación o extracción de la misma.