Declaración de Prácticas de Certificación
PSC World, S.A. de C.V.
Prestador de Servicios de Certificación

Tabla de Contenido

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 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.

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 las Agencias de Registro (AR) y los Agentes de Certificación acreditadas por **PSC World**.

Al emitir un certificado digital, una Autoridad 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 autoridad certificadora para emitir dicho certificado, es decir, las ***Prácticas de Certificación***. Asimismo, también es relevante poder distinguir que práctica es mejor que otra, así como el grado de reconocimiento que dichas prácticas puedan tener en distintas comunidades y ambientes.

Por otro lado, para poder comparar es necesario que exista algún punto de referencia común que guíe la evaluación. Es por eso que **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, tales como el estándar ETSI TS 102 042 y el RFC 3647.

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

2. Definiciones

Certificado: Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
Datos de Creación de Firma Electrónica: Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
Destinatario: La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje.
Emisor: Toda persona que, al tenor del Mensaje de Datos, haya actuado a nombre propio o en cuyo nombre se haya enviado o generado ese mensaje antes de ser archivado, si éste es el caso, pero que no haya actuado a título de Intermediario.
Firma Electrónica: Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
Firma Electrónica Avanzada o Fiable: Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97.
En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.
Firmante: La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa.
Intermediario: En relación con un determinado Mensaje de Datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho Mensaje o preste algún otro servicio con respecto a él.
Mensaje de Datos: La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.
Parte que Confía: La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.
Secretaría: Se entenderá la Secretaría de Economía.
Prestador de Servicios de Certificación: La persona o institución que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso.
Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma Mensajes de Datos.
Solicitante: Se entenderá a la persona que tramita la Solicitud de Certificado
Titular: Se entenderá a la persona a cuyo favor fue expedido el Certificado.
Agente Certificador: A la institución o persona física que verifica la identidad de los Solicitantes
Agencia Certificadora: A la institución que presta servicios de certificación mediante la expedición de Certificados Digitales
Agencia Registradora: A la institución autorizada para llevar el registro electrónico de los Certificados Digitales expedidos por la Agencia Certificadora

←Regresar

3. Alcance

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.

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
- 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 las Agencias Certificadoras, Agencias de Registros, Agentes Certificadores y Solicitantes, para la emisión de Certificados por **PSC World,** de acuerdo con cada tipo de certificado y las limitaciones de uso establecidas para cada caso.

Los Certificados, 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 o un Fedatario. 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.

←Regresar

4. Tipos y Contenido de los Certificados emitidos por PSC World

4.1. Tipos de 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. Representación de empresas – El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas con actividad empresarial o personas morales para garantizar frente a terceros su identidad, autenticidad e integridad de sus mensajes, así como que el representante legal de una empresa manifieste que su representada se encuentra capacitada legalmente para la celebración del acto y acreditar que la personalidad que ostenta y las facultades con que cuenta no le han sido limitadas, modificadas o revocadas.
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.
4. Certificado de Correo Electrónico – El certificado tendrá como única finalidad asegurar la existencia y denominación del signatario del certificado. Estos certificados serán emitidos a personas físicas para garantizar ante terceros su identidad, autenticidad e integridad de los mensajes mediante aplicaciones de correo electrónico seguro S/MIME, para cifrar y firmar mensajes.

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	▪ Requiere presencia personal de un 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	▪ Autenticación de servidor ▪ Comercio electrónico
Representación de empresas	▪ Requiere presencia personal de un representante legal de la empresa para acreditar la	▪ Comercio electrónico ▪ Servicios de suscripción ▪ Correo electrónico seguro

	personalidad de la representada ▪ Se registra documentación y firma autógrafa	S/MIME ▪ Autenticación en sitio Web ▪ Firma de documentos ▪ Firma de contratos
Certificado personal	▪ Requiere presencia personal para acreditar la identidad ▪ Se registra documentación y firma autógrafa	▪ Comercio electrónico ▪ Servicios de suscripción ▪ Correo electrónico seguro S/MIME ▪ Autenticación en sitio Web ▪ Firma de documentos ▪ Firma de contratos
Certificado de correo electrónico	▪ Requiere presencia personal para acreditar la identidad ▪ Se registra documentación y firma autógrafa	▪ Correo electrónico seguro S/MIME

4.2. 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
Datos de acreditación ante la Secretaria
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 Secretaria especifique.

←Regresar

5. Procedimiento de Operación

5.1. Requerimiento de Solicitud de Certificado Digital

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

I. Persona Física

a. Descargar el ***Manual de Obtención de Certificado vía Web.*** Este manual describe los prerrequisitos necesarios para realizar la solicitud del certificado digital y un manual de usuario, que describe de manera detallada los pasos a seguir para la generación de las llaves y el certificado.
   i. Descargar el ***Manual de Obtención de Certificado vía Web*** en la ruta www.pscworld.com
   ii. Leer detalladamente las instrucciones

b. Descargar y completar el ***Requerimiento de Solicitud de Certificado Digital***. 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.
   i. Descargar el ***Requerimiento de Solicitud de Certificado Digital*** en la ruta www.pscworld.com
   ii. Imprimir Requerimiento de Solicitud de Certificado Digital
   iii. Cumplir con los requisitos previos de entrega del Requerimiento de ***Solicitud de Certificado Digital***
   iv. Requisitar ***Requerimiento de Solicitud de Certificado Digital***

c. Generar ***Requerimiento de Certificación*** en la ruta www.pscworld.com . En este proceso el **Solicitante** genera su par de llaves (pública y privada) a través del Servicio de Certificación Web de PSC World. Los requerimientos mínimos son:
   i. Computadora personal con sistema operativo Windows 98 / 2000 / ME / XP (con todos los parches y actualizaciones instalados)
   ii. Microsoft Internet Explorer 5.5 o superior (con todos los parches instalados)
   iii. Conexión a Internet

   La llave privada se mantiene localmente en el equipo de cómputo del Solicitante mientras que la llave pública es enviada a la Agencia Certificadora de **PSC World** como ***Requerimiento de Certificación***. Para realizar este proceso se requiere completar los siguientes pasos:
   i. Acceder a la opción *Generar Requerimiento de Certificación* del menú Servicios de Certificación Electrónica
   ii. Llenar la forma con los datos solicitados, necesarios para crear el par de llaves.
   iii. Seleccionar el nivel de seguridad, se recomienda establecer el mismo en Alto (High).
   iv. Generar las llaves

   La llave privada quedará en el repositorio de llaves de Microsoft Internet Explorer y el requerimiento será enviado el Agente Certificador para su posterior procesamiento.

d. Imprimir el ID del requerimiento, que se obtiene al terminar el proceso de generación del Requerimiento de Certificación, para su presentación ante el Agente Certificador

e. Presentar documentación ante un Agente Certificador autorizado por PSC World.

i. Podrá acceder a la lista de los Agentes Certificadores autorizados por PSC World en la ruta www.pscworld.com
ii. Presentar original y copia para cotejo de los siguientes documentos:
    1. Identificación oficial vigente (credencial para votar, pasaporte o cédula profesional)
    2. Dos comprobantes de domicilio actual, con una antigüedad no mayor a un mes, tal como (recibo telefónico, luz o estados de cuenta de instituciones del sistema financiero, casas comerciales o tarjetas de crédito no bancarias)
    3. Formulario de Solicitud de Certificado Digital

II. Persona Moral

a. Descargar el ***Manual de Obtención de Certificado vía Web***. Este manual describe los prerrequisitos necesarios para realizar la solicitud del certificado digital y un manual de usuario, que describe de manera detallada los pasos a seguir para la generación de las llaves y el certificado.
    i. Descargar el ***Manual de Obtención de Certificado vía Web*** en la ruta www.pscworld.com
    ii. Leer detalladamente las instrucciones
b. Descargar y completar el ***Requerimiento de Solicitud de Certificado Digital***. 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.
    i. Descargar el ***Requerimiento de Solicitud de Certificado Digital*** en la ruta www.pscworld.com
    ii. Imprimir Requerimiento de Solicitud de Certificado Digital
    iii. Cumplir con los requisitos previos de entrega del Requerimiento de ***Solicitud de Certificado Digital***
    iv. Requisitar Requerimiento de Solicitud de Certificado Digital
c. Generar Requerimiento de Certificación en la ruta www.pscworld.com. En este proceso el **Solicitante** genera su par de llaves (pública y privada) a través del Servicio de Certificación Web de PSC World. Los requerimientos mínimos son:
    i. Computadora personal con sistema operativo Windows 98 / 2000 / ME / XP (con todos los parches y actualizaciones instalados)
    ii. Microsoft Internet Explorer 5.5 o superior (con todos los parches instalados)
    iii. Conexión a Internet

    La llave privada se mantiene localmente en el equipo de cómputo del Solicitante mientras que la llave pública es enviada a la Agencia Certificadora de PSC World como Requerimiento de Certificación. Para realizar este proceso se requiere completar los siguientes pasos:
    i. Acceder a la opción *Generar Requerimiento de Certificación* del menú Servicios de Certificación Electrónica
    ii. Llenar la forma con los datos solicitados, necesarios para crear el par de llaves.

iii. Seleccionar el nivel de seguridad, se recomienda establecer el mismo en Alto (High).
iv. Generar las llaves

La llave privada quedará en el repositorio de llaves de Microsoft Internet Explorer y el requerimiento será enviado el Agente Certificador para su posterior procesamiento.

d. Imprimir el ID del requerimiento, que se obtiene al terminar el proceso de generación del Requerimiento de Certificación, para su presentación ante el Agente Certificador.
e. Presentar documentación ante un Agente Certificador autorizado por PSC World.
   i. Podrá acceder a la lista de los Agentes Certificadores autorizados por PSC World en la ruta www.pscworld.com
   ii. Presentar original y copia para cotejo de los siguientes documentos:
      1. Acta constitutiva
      2. Escrituras de reformas a la constitutiva
      3. Poder notarial del representante legal
      4. Identificación oficial vigente del representante legal (credencial para votar, pasaporte o cédula profesional)
      5. Alta ante la Secretaria de Hacienda y Crédito público
      6. Cédula del Registro Federal de Contribuyentes
      7. Comprobante de domicilio actual (boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial)

5.2. El Agente Certificador tendrá la obligación de:

II. Certificar la identidad del Solicitante
III. Verificar y corroborar la información contenida en el Requerimiento de Solicitud de Certificado Digital con base en los documentos solicitados
   a. De existir alguna discrepancia entre la documentación solicitada para cotejo y la información registrada en el Requerimiento de Solicitud de Certificado Digital, 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.
IV. Procesar los Requerimientos de Certificación. Para poder realizar este proceso, el Agente Certificador, deberá contar con un certificado emitido por la Agencia Certificadora y registrado como Agente válido ante PSC World.
   a. Generar precertificado. En este proceso el Agente de Registro firma digitalmente el requerimiento del Solicitante y lo transmite a la Agencia Certificadora. Para realizar este proceso se requiere completar los siguientes pasos:
      i. Entrar número de serie que le fue proporcionado al Solicitante al realizar la Solicitud de Certificado, para recuperar el requerimiento.
      ii. Seleccionar las características del certificado que será generado
      iii. Realizar certificación del requerimiento

b. Entregar al **Solicitante** Recibo de Emisión del Certificado, una vez generado por la Agencia Certificadora
c. El Solicitante tendrá que firmar el ***Recibo de Emisión del Certificado*** y el ***Acuerdo de Prestación de Servicios.***

V. El Agente Certificador 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

5.3. La Agencia Certificadora tendrá la obligación de:

I. Recibir el precertificado y validar la firma electrónica del Agente Certificador y del **Solicitante**.
II. Emitir un Certificado Digital con su firma electrónica.
III. Enviar el certificado a la Agencia Registradora para su registro.
IV. Enviar el certificado ya registrado en la Agencia Registradora al Agente Certificador para que a su vez entregue el recibo de emisión al **Solicitante**
V. La Agencia Certificadora 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

5.4. El Solicitante tendrá la obligación de:

I. Descargar certificado en la ruta www.pscworld.com

←Regresar

6. Responsabilidades y obligaciones

6.1. PSC World

PSC World asume el cumplimiento de las obligaciones que le impone la legislación aplicable, las normas y decretos establecidos por:

SECRETARIA DE ECONOMIA

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

6.2. Obligaciones y responsabilidades de los Agentes Certificadores

I. Verificar la identidad de los individuos que desean obtener certificados digitales.
II. Verificar y corroborar la información contenida en el Requerimiento de Solicitud de Certificado Digital con base en los documentos solicitados
III. Garantizar que el solicitante cumpla con los requisitos establecidos en la presente

Declaración de Prácticas de Certificación

IV. Procesar los requerimientos de certificación

V. Los Agentes Certificadores responderán ante la ***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 presente ***Declaración de Prácticas de Certificación***

6.3. Obligaciones y responsabilidades de PSC World como Agencia Certificadora

I. Recibir los precertificados y validar la firma electrónica de los Agentes Certificadores y de los **Solicitantes**.

II. Emitir Certificados Digitales con su firma electrónica.

III. Enviar los certificados a las Agencias Registradoras para su registro.

IV. Enviar los certificados ya registrados en la Agencia Registradora al Agente Certificador para que a su vez entregue el recibo de emisión al **Solicitante**

V. Crear los certificados digitales de los Agentes Certificadores y/o acreditarlos como tales.

VI. Generar las Listas de Revocación

VII. La Agencia Certificadora se reserva el derecho a no emitir certificados cuando así lo estime conveniente, sin que por ello pueda exigirse responsabilidad alguna

VIII. Solicitar revocaciones cuando los Agentes Certificadores o usuarios lo soliciten.

IX. Hacer las funciones de Agente Certificador cuando sea necesario.

X. La Agencia Certificadora será responsable únicamente de la información contenida en los certificados por ella emitidos y durante el periodo en que los mismos mantengan su vigencia.

XI. La Agencia Certificadora no será responsable de los daños y perjuicios que puedan deducirse por motivo de la utilización de un certificado por ella emitido.

XII. La Agencia Certificadora no responderá de los daños y perjuicios que se deriven de actuaciones negligentes o dolosas por parte de terceros con relación a los certificados por él emitidos.

XIII. La Agencia Certificadora no responderá de la utilización del certificado para usos distintos de aquellos para los cuales se haya emitido.

XIV. La Agencia Certificadora no asumirá responsabilidad alguna por la no ejecución o el retraso en la ejecución de cualquiera de las obligaciones previstas en la presente ***Declaración de Prácticas de Certificación***, si tal falta de ejecución o retraso resultara o fuera consecuencia de un supuesto de fuerza mayor, caso fortuito o cualquier circunstancia sobre la que la Agencia Certificadora no pueda tener un control razonable.

XV. La Agencia Certificadora no será responsable del contenido de los documentos firmados digitalmente ni de las páginas Web que contengan un certificado por ella emitido.

6.4. Obligaciones y responsabilidades de PSC World como Agencia Registradora

I. Registrar certificados digitales siempre y cuando la Agencia Registradora Central confirme la unicidad de las llaves públicas.
II. Administrar las bases de datos con los certificados digitales registrados, tanto actuales como históricas.
III. Proporcionar los certificados digitales que le soliciten los usuarios a través de medios electrónicos.
IV. Revocar certificados digitales y divulgar dichas revocaciones.
V. Garantizar la integridad de las Listas de Revocación
VI. Conservar toda la información y documentación relativa a los certificados

6.5. Obligaciones y responsabilidades de los Solicitantes

I. Establecer su frase de seguridad y generar su par de claves (pública y privada).
II. Solicitar su certificado digital a través de un Agente Certificador o Fedatario, presentando su ***Requerimiento de Solicitud de Certificado Digital***
III. Conocer y aceptar las normas estipuladas en el contrato con **PSC World**
IV. Descargar su certificado digital ya registrado.
V. Mantener en un lugar seguro su clave privada.
VI. No olvidar la frase de seguridad y mantenerla en secreto.
VII. Notificar a **PSC World** de cualquier modificación de sus antecedentes, que como consecuencia pudiera invalidar uno o más certificados emitidos a su nombre.
VIII. Cumplir las obligaciones derivadas del uso de la Firma Electrónica;
IX. Actuar con diligencia y establecer los medios razonables para evitar la utilización no autorizada de los Datos de Creación de la Firma;
X. 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 mismo, son exactas.
XI. El Firmante será responsable de las consecuencias jurídicas que deriven por no cumplir oportunamente las obligaciones previstas en el presente artículo,
XII. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el Destinatario conociere de la inseguridad de la Firma Electrónica o no hubiere actuado con la debida diligencia.

←Regresar

7. Vigencia de los certificados y procedimientos de revocación

7.1. Vigencia

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

I. Expiración del periodo de vigencia del Certificado, el cual no podrá ser superior a dos años, contados a partir de la fecha en que se hubieren expedido. Antes de que

concluya el periodo de vigencia del Certificado podrá el Firmante renovarlo ante el Prestador de Servicios de Certificación.

II. Revocación por el Prestador de Servicios de Certificación, a solicitud del Firmante, o por la persona física o moral representada por éste o por un tercero autorizado.
III. Pérdida o inutilización por daños del dispositivo en el que se contenga dicho Certificado.
IV. 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.
V. Resolución judicial o de autoridad competente que lo ordene.
VI. Cuando la seguridad de la clave privada se haya comprometido
VII. Cuando se haya producido un error en la emisión del certificado debido a una falta de adecuación en el procedimiento establecido
VIII. Cuando el **Solicitante** incumpla las condiciones de utilización de los certificados establecidas en el contrato con **PSC World.**

7.2. Procedimientos para solicitar la revocación de un certificado

I. El Titular puede realizar la revocación a través del ***Servicio de Certificación vía Web,*** en la ruta www.pscworld.com
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.

7.3. 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 on-line mediante el uso del Web en www.pscworld.com

II. La información respecto a la revocación de un certificado quedará disponible en el sitio Web inmediatamente después de completado el proceso de la solicitud de revocación.
III. Las listas de Certificados Revocados serán actualizadas con una frecuencia de 12 horas entre cada publicación.

←Regresar

8. Método de verificación de identidad del usuario

La verificación de la identidad del **Solicitante** se realizará en el ***Proceso de Registro***

I. Se requerirá la presencia ante un Agente Certificador autorizado por PSC World, el **Solicitante** tendrá que presentar original y copia para cotejo de los siguientes documentos:
    a. Persona Física
        i. Identificación oficial vigente; credencial para votar, pasaporte o cédula profesional
        ii. Comprobante de domicilio actual; boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial
    b. Persona Moral
        i. Acta constitutiva
        ii. Poder notarial del representante legal
        iii. Identificación oficial vigente del representante legal (credencial para votar, pasaporte o cédula profesional)
        iv. Alta ante la Secretaria de Hacienda y Crédito público
        v. Cédula del Registro Federal de Contribuyentes
        vi. Comprobante de domicilio actual (boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial)
        vii. Requerimiento de Solicitud de Certificado Digital
II. El Agente Certificador certificará la identidad del Solicitante corroborando la información contenida en el ***Requerimiento de Solicitud de Certificado Digital*** con base en los documentos solicitados
    a. El Agente Certificador comprobará la razonable coincidencia entre la fotografía contenida en el documento de Identificación Oficial y la apariencia física del **Solicitante**
III. Dicha presencia se registrará mediante la firma ológrafa en el ***Contrato de Prestación de Servicios***.
IV. De existir alguna discrepancia entre la documentación solicitada para cotejo y la información registrada en el Requerimiento de Solicitud de Certificado Digital, la solicitud será rechazada.
V. El Agente Certificador y la Agencia de Certificación, 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.
VI. Los Agentes Certificadores y la Agencia de Certificación, 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

←Regresar

9. Protección de confidencialidad y seguridad de la información.

I. PSC Word se rige por su ***Política de Privacidad*** para la protección de la confidencialidad de la información.
II. PSC World deja claramente establecido que no comparte, vende, cede, ni transfiere la información personal de los usuarios.
III. Para proteger la información de sus clientes, PSC World ha establecido un conjunto de políticas y procedimientos de seguridad de acceso a la información
IV. PSC World utiliza los servicios de seguridad que brinda Prodigy Data Center www.triara.com/centrodatos.htm

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, se encuentra el Prodigy Data Center de Telmex, 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 Seguridad Física"***, y los controles 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.

Seguridad Física

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

Seguridad Lógica

- Múltiple tecnología de firewall
- Sistema de detección de intrusos
- Sistemas de análisis de seguridad activos

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 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.

Sistema de Control Ambiental

El sistema ambiental del 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. El Prodigy Data Center utiliza también aires de precisión en los componentes críticos de la infraestructura de energía eléctrica.

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 esta manera, el personal del Centro 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.

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

←Regresar

10. 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**.

←Regresar

11. 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 **Secretaria** para garantizar la redundancia del servicio.

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 descrito en el apartado 5 anterior de estas Reglas Generales.

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 **PSC World** entregará en medio óptico o electrónico respaldo de la base de datos de los certificados a la Secretaria de Economía o Prestador de Servicios de Certificación por este designado. Dicho acto de respaldo y entrega será protocolizado ante notario público.

←Regresar

12. 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.**

←Regresar

13. Controles que se utilizan para asegurar:

13.1. 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 generación del **Requerimiento del Certificado** a través del **Servicio de Certificación Web 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 Navegador Web.

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

←Regresar

13.2. Autenticación de usuarios

La autenticación de los usuarios de PSC World que tramita la Solicitud de un Certificado se realiza a través de los **Agentes Certificadores** acreditados por **PSC World**.

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

1. **Agentes Certificadores Fedatarios Públicos**: Son Notarios o Corredores Públicos acreditados por PSC World y que emiten certificados con fe pública.
2. **Agentes Certificadores PSC World:** Son personas físicas o morales acreditados por PSC World que emiten certificados sin fe pública.

Para garantizar la autenticación de los usuarios, el **Agente Certificador** está obligado a cumplir con el procedimiento descrito en el apéndice 5.1 de este documento, cotejando la firma y fisonomía del solicitante con los documentos solicitados.

←Regresar

13.2.1. Autenticación de 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 **Solicitante** para acreditación, tendrá que presentar original y copia para cotejo de los siguientes documentos:

Notario Público

- Identificación oficial vigente; credencial para votar, pasaporte o cédula profesional
- Comprobante de domicilio actual; 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
- Comprobante de domicilio actual; boleta predial, recibo telefónico, luz, agua o cualquier otro comprobante oficial.
- Habilitación para ejercer como Corredor Público

←Regresar

13.3. 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 servicio que permiten una alta disponibilidad de los mismos y 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

←Regresar

13.4. 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 de este documento.

El constante monitoreo de los niveles de servicio de la infraestructura tecnológica de **PSC World**, es un control de 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.

←Regresar

13.5. 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:

I. Autenticar los registros de la base de datos.
II. Generar reportes de actividad.

←Regresar

13.6. 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.

←Regresar