Documento

Declaración de Prácticas de Certificación de la Autoridad Certificadora

PSC Codex

Versión 1.1

2 de septiembre del 2022

Tabla de contenido

Antecedentes

El comercio electrónico ha sido un detonante en la productividad de los mercados durante los últimos años como una forma de hacer negocios y comunicarse a través de todo tipo de redes de comunicación, donde la simplificación de las interacciones entre los participantes resulta fundamental. Pero para que estar interacciones realmente puedan simplificarse, es indispensable que todos los actores se encuentren identificados y que se cuente con los medios y mecanismos suficientes para proteger la confidencialidad de los datos que se intercambian, así como que los mismos no sean alterados con posterioridad a que se realiza la acción o transacción.

En México, estos requerimientos se pueden dar cumplidos si se integran los servicios que ofrecen los Prestadores de Servicios de Certificación, entre los que destaca la emisión de certificados digitales, en este caso emitidos por la Autoridad Certificadora de PSC Codex. Estos certificados son originados utilizando algoritmos criptográficos que respaldan la operación de la Autoridad Certificadora y, a partir de ello, respaldan las acciones o transacciones que se realizan por medio de ellos.

Ahora bien, para que los participantes del comercio electrónico puedan tener confianza en la seguridad de los mecanismos criptográficos, los Prestadores de Servicios de Certificación requieren ser acreditados por la Secretaría de Economía mediante un proceso administrativo en el cual deben demostrar que han establecido procedimientos y medidas de protección adecuadas para minimizar las amenazas y riesgos operativos y financieros asociados con los sistemas criptográficos de clave pública.

Dentro de esos requisitos, se encuentra la elaboración y publicación de la Declaración de Prácticas de Certificación de la Autoridad Certificadora de PSC Codex, la cual tiene como objetivo divulgar los procedimientos y procesos que PSC Codex ha establecido como parte del proceso de generación de certificados digitales para sus suscriptores. La Declaración de Prácticas busca ser la guía de conocimiento para suscriptores y partes interesadas respecto de los procesos asociados a la Autoridad Certificadora de PSC Codex.

Fuentes

- Ley de Firma Electrónica Avanzada
- Código de Comercio
- Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
- Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares

Glosario de Términos

Concepto	Descripción
Certificado	Llave pública del usuario que, en conjunto con la llave privada y la frase de seguridad, componen un elemento imposible de falsificar al ser cifrados con la clave privada de la AC que los emitió.
CRL	Listado firmado por la Autoridad certificadora que la emite en la cual se relacionan los certificados digitales que ya no son considerados como válidos.
Firma electrónica	Datos en formato electrónico que se adjuntan o se asocian lógicamente con otros datos electrónicos y que sirven como método de autenticación de esos datos.
PSC Codex	Nombre de la empresa que inicia su emprendimiento como Prestador de Servicios de Certificación bajo la NORMA Oficial Mexicana NOM-151-SCFI-2016

Framework de referencia

PSC Codex ha desarrollado la presente Declaración de Prácticas de Certificación de su Autoridad Certificadora tomando como referencia los conceptos, rubros y características que se mencionan dentro de las especificaciones técnicas del estándar ETSI TS 102 042 V2.1.2 que tiene como título "*Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*". Este documento tiene como finalidad establecer los lineamientos mínimos que deben de cumplir las organizaciones en la emisión de la Declaración de Prácticas de los servicios relativos a la emisión de certificados digitales, lo anterior con la finalidad de que los suscriptores y partes interesadas tengan pleno conocimiento respecto de la forma en que será prestado el servicio, así como de la delimitación de obligaciones y responsabilidades específicas para cada una de las partes.

Siguiendo este estándar PSC Codex, como Prestador de Servicios de Certificación, dentro del presente documento establecerá la información requerida para los siguientes apartados:

1. Conceptos Generales del servicio.
2. Política de certificados.
3. Ciclo de vida de las llaves criptográficas
4. Obligaciones y responsabilidades.

Conforme lo señalan las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, a lo largo del presente documento se desarrollarán cada uno de estos apartados, así como aquellos que no fueron mencionados en el listado y que son mencionados dentro del ETSI TS 102 042 V2.1.2.

Es importante señalar que la presente Declaración de Prácticas es compatible con el Rfc 3647 al desarrollar los apartados que señala el Rfc mencionado y cuya relación con los apartados desarrollados por el ETSI TS 102 042 V2.1.2 pueden visualizarse en el Anexo C del ETSI de referencia.

Conceptos Generales

Autoridad Certificadora

Una autoridad certificadora es el organismo o entidad en la que confían los usuarios de servicios de confianza, suscriptores y partes interesadas, para la emisión de certificados digitales utilizados principalmente para la firma electrónica de mensajes de datos. La autoridad certificadora tiene a su cargo los servicios de certificación que permiten utilizar los certificados digitales en entornos seguros y ofreciendo diversas herramientas a sus suscriptores para el uso y aprovechamiento de estos.

Dentro de los certificados digitales, la autoridad certificadora será identificada como el emisor de los certificados que se emiten y que están subordinados a la misma, además de que dichos certificados serán firmados por la llave privada de la autoridad certificadora.

Servicios de certificación

Una de las responsabilidades de la Autoridad Certificadora es la de proporcionar y tener disponibles diversos componentes y servicios que en el entorno de la Infraestructura de Clave Pública permitan el correcto funcionamiento de los certificados que ha emitido. Entre los servicios a destacar que proporciona la Autoridad Certificadora de PSC Codex, se encuentran:

1. Servicio de registro. Es el proceso mediante el cual la Autoridad Certificadora recopila la información del interesado en obtener un certificado digital, además de verificar y garantizar que la identidad del interesado es legítima utilizando diversos servicios y mecanismos de validación de identidad.
2. Servicio de generación de certificados. Como parte de este servicio se realiza el proceso de creación, asignación y firma del certificado por parte de la Autoridad Certificadora una vez que la identidad y documentación del interesado han sido validados. El proceso de generación de certificados únicamente puede ser ejecutado por el o los agentes certificadores acreditados por PSC Codex ante la Secretaría de Economía.
3. Servicio de distribución. Es el servicio mediante el cual se hace de conocimiento de la Secretaría de Economía la llave pública de los certificados digitales que PSC Codex como Autoridad Certificadora emita. Este servicio también es el encargado de publicar los términos y condiciones de operación de la Autoridad Certificadora, así como las Políticas de Certificación y la Declaración de Prácticas de Certificación. El servicio de distribución estará disponible principalmente en la página de internet de PSC Codex. https://www.psccodex.com/practicas_certificados/
4. Servicio de revocación de certificados. Servicio a través del cual los interesados poseedores de un certificado digital emitido por la Autoridad Certificadora de PSC Codex podrán solicitar la revocación de dicho certificado atendiendo a las condiciones que se describen en el presente documento.
5. Servicio de validación del estatus del certificado. PSC Codex implementa dos servicios que permiten a los suscriptores y partes interesadas verificar el estatus

de un certificado. Para ello provee una CRL que se actualiza en plazos no mayores a 24 horas, además de tener habilitado el protocolo OCSP para la validación en tiempo real del estatus del certificado.

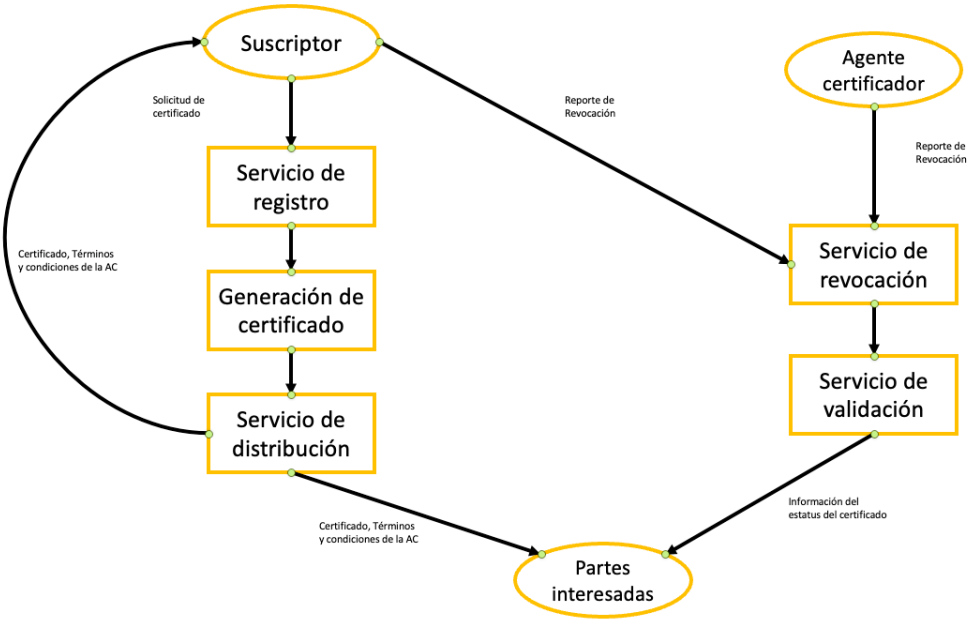

Ilustración 1 Relación de los servicios de la Autoridad Certificadora

Suscriptores

PSC Codex define a sus suscriptores como todas aquellas personas físicas que requieren de la emisión de certificados digitales para poder participar en procesos de firma electrónica avanzada como parte de los procesos de su organización, actividad o interacciones con terceros. Los interesados en el servicio se convierten en suscriptores cuando dan cumplimiento a los requisitos que ha establecido PSC Codex para la emisión de certificados digitales y el proceso de emisión del certificado se concluye satisfactoriamente. Una vez emitido el certificado, el suscriptor adquiere las obligaciones y responsabilidades que se describen en el presente documento respecto del uso del certificado digital.

Las personas físicas interesadas en ser suscriptores del servicio deberán cumplir con los requisitos y documentación siguientes:

Tratándose de personas físicas nacidas en territorio mexicano:

1. Ser mayor de edad
2. Acta de nacimiento.
3. Identificación oficial vigente (INE, Pasaporte, Cédula profesional).
4. CURP
5. RFC.
6. Comprobante domicilio no mayor a 3 meses.

Tratándose de personas físicas nacidas en el extranjero:

1. Pasaporte emitido por el país de origen, el cual deberá encontrarse vigente.
2. Documento oficial expedido por el Instituto Nacional de Migración (Cuando cuente con él, que acredite su internación o legal estancia en el país) FM2 o FM3
3. Comprobante de domicilio no mayor a 3 meses
4. RFC.

Sujetos relacionados

Como ya se estableció, el suscriptor del servicio de emisión de certificados digitales es la persona física o moral que realiza la contratación del servicio. Ahora bien, los sujetos relacionados son definidos por PSC Codex como las personas físicas relacionadas directa o indirectamente para quien una persona moral solicita la emisión de un certificado. Si bien, la persona moral es la que adquiere las obligaciones y responsabilidades del uso del certificado, los sujetos relacionados se vuelven responsables solidarios al ser quienes serán autenticados y harán uso del certificado digital emitido. El certificado que se proporciona a un sujeto relacionado contiene los datos asociados a su identidad y solo debe de ser utilizado por el individuo a quien fue emitido dicho certificado.

Las personas morales que requieran de la emisión de un certificado digital a un sujeto relacionado, además de la solicitud correspondiente, deberán cumplir con los requisitos y documentación que se establecen para los suscriptores del servicio.

Política de Certificación

Visión General de la Política

Las políticas de certificación, así como la declaración de prácticas de certificación de la Autoridad Certificadora de PSC Codex, tienen como finalidad establecer los procedimientos, obligaciones, responsabilidades, limitantes, entre otros, a que se hacen sujetos aquellos suscriptores del servicio de emisión de certificados digitales de PSC Codex. Ambos elementos son identificados a través de un OID emitido por la Secretaría de Economía el cual debe de ser incluido dentro de los certificados emitidos con lo cual suscriptores y partes interesadas expresan su aceptación por las políticas y declaraciones de certificación.

La Política de Certificación de PSC Codex puede considerarse como una Política NCP que es particularmente adecuada para soportar servicios de firma electrónica avanzada como se define en la Directiva de Firma Electrónica (1999/93/EC).

Identificación del documento

La Política de Certificación de la Autoridad Certificadora de PSC Codex puede ser identificada a través del OID que asigna la Secretaría de Economía cuando se concluye satisfactoriamente con el proceso de acreditación como Prestador de Servicios de Certificación para el servicio de emisión de Certificados Digitales.

El identificador asignado por la Secretaría a la Política de Certificación de PSC Codex esta estructurado conforme al estándar X.208 descrito en el RFC 3628 y que entre otras cuestiones permite identificar a la organización acreditada, la organización que emite la acreditación, la versión de la política, así como el servicio para el cual se emite dicha política. El OID asignado a PSC Codex para su Política de Certificación, será incluido en la Autoridad Certificadora de PSC Codex y, por ende, en cada uno de los certificados digitales emitidos por dicha autoridad.

OID de la Política Certificación de la AC de PSC Codex: [Pendiente de asignación por parte de la Secretaría de Economía].

Inicio de operaciones

Con fecha de 07 de marzo del año 2023 la Secretaría de Economía resolvió otorgar la acreditación como Prestador de Servicios de Certificación a PSC Codex para el servicio de emisión de Certificados Digitales, publicando en el Diario Oficial de la Federación la acreditación correspondiente el 24 de marzo del año 2023

Publicada la acreditación, PSC Codex inicio operaciones del servicio de emisión de Certificados Digitales con fecha [Pendiente de dictamen de la SE].

Publicación de la Declaración de Prácticas

PSC Codex pone a disposición de suscriptores y partes interesadas la versión digital de la Declaración de Prácticas de Certificación, la cual, al considerarse como un documento de acceso público estará disponible en la dirección electrónicahttps://www.psccodex.com/practicas_certificados/.

Usuarios y aplicabilidad

La presente Política de Certificación cumple con los requerimientos que se establecen en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación con relación a la estructura y contenido que deben de considerarse como parte del proceso de registro y emisión de certificados digitales por la Autoridad correspondiente y atendiendo a la definición y alcance que se establece para los Prestadores de Servicios de Certificación dentro del Código de Comercio y la Ley de Firma Electrónica Avanzada.

Tecnológicamente esta Política establece los lineamientos a través de los cuales se da cumplimiento a los requerimientos para la emisión de certificados digitales de firma electrónica avanzada conforme a la Directiva Europea de Firma Electrónica, definidas en el ETSI TS 102 042 V2.1.2.

Esta política será aplicable a la comunidad de usuarios del servicio de emisión de certificados digitales que proporciona PSC Codex, entendiendo como comunidad de usuarios a los suscriptores del servicio, así como a las partes interesadas en el mismo. La Política de Certificación de la Autoridad Certificadora es considerada como un documento de acceso público por parte de PSC Codex por lo que será consultable en la dirección https://www.psccodex.com/practicas_certificados/.

Conformidad

Declaración de conformidad

PSC Codex declara que conforme lo establece el RFC 5280 su Autoridad de Certificadora incluye dentro de los certificados digitales que emite el OID que le ha sido asignado por la Secretaría de Economía, una vez que le ha sido otorgada la acreditación como PSC para el servicio de emisión de Certificados Digitales.

El OID que se incluye en los Certificados Digitales es: [Pendiente de asignación por la SE]

PSC Codex hará del conocimiento de los suscriptores y partes interesadas en el servicio de emisión de Certificados Digitales el OID asignado por la Secretaría y será consultable dentro de la Política de Certificación y en la presente Declaración de Prácticas de Certificación de la Autoridad Certificadora.

Obligaciones y responsabilidades

Los participantes de la emisión de certificados digitales, tanto PSC como Prestador de Servicios de Certificación, como los suscriptores, sujetos relacionados y partes interesadas conocen, aceptan y asumen las obligaciones y responsabilidades que se generan como parte del servicio. Cada uno de los participantes mencionados deberá cumplir con las obligaciones que se establecen en el presente documento y que forman parte del documento de términos y condiciones del servicio.

La inobservancia u omisión de obligaciones y responsabilidades, así como el mal uso del certificado pueden derivar en la suspensión del servicio y, por tanto, en la revocación del certificado digital emitido.

Obligaciones de la AC de PSC Codex

Obligaciones generales

PSC Codex como Prestador de Servicios de Certificación acreditado por la Secretaría de Economía tiene la obligación de cumplir con los criterios y requerimientos que se establecen en la normatividad aplicable a fin de brindar servicios de certificación confiables y que en todo momento privilegien las tres principales características de la seguridad de la información como son la integridad, confidencialidad y disponibilidad.

Entre las principales obligaciones que PSC Codex cumple, se encuentran las siguientes:

a) Contar con un seguro de responsabilidad civil para cada año y durante el tiempo que permanezca acreditado como Prestador de Servicios de Certificación.
b) Contar con una fianza para cada año y durante el tiempo que permanezca acreditado el Prestador de Servicios de Certificación.
c) Contar con el espacio físico, controles de seguridad, accesos, perímetros de seguridad física, medidas de protección y políticas necesarias para garantizar la seguridad para la emisión de Certificados Digitales.
d) Contar con una oficina administrativa sujeta a los procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.
e) Contar con dos centros de datos, uno principal y otro alterno, que deberán cumplir con las certificaciones y estándares de calidad y seguridad, así como contar con procedimientos y prácticas de seguridad firmados por el Profesional Jurídico, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.
f) Contar con los elementos humanos, económicos, materiales y tecnológicos requeridos en el Título Quinto de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de certificación.
g) Notificar a la Secretaría de Economía respecto de la emisión de cada uno de los certificados digitales que emita la AC de PSC Codex, en conformidad con el procedimiento que establezca la propia Secretaría.

Obligaciones de la AC con sus suscriptores

Además de las obligaciones que tiene PSC Codex inherentes a su actuar como Prestador de Servicios de Certificación, la organización con la finalidad de brindar un servicio de confianza y calidad para sus suscriptores ha establecido una serie de obligaciones para su servicio de emisión de certificados digitales.

Estas obligaciones están directamente relacionadas con sus suscriptores y los compromisos que tiene PSC Codex con ellos.

a) Establecer los medios necesarios para que los interesados en la generación de un certificado digital puedan ingresar y verificar directamente la información que se integrará al certificado digital.
b) Contar con un sitio electrónico de alta disponibilidad en el cual los usuarios puedan consultar la clave pública de los certificados que les han sido emitidos.
c) Implementar procesos de verificación de identidad adecuados que permitan relacionar de forma fehaciente la identidad del usuario que solicita la emisión del certificado digital. Este proceso se realizará conforme se describe en el apartado "*Verificación de identidad*" del presente documento.
d) PSC Codex eliminará la llave privada del certificado digital emitido una vez que el mismo ha sido entregado a satisfacción del solicitante. El personal de PSC Codex, incluyendo al agente certificador y Autoridad Registradora, no resguardarán ni podrán recuperar la llave privada de los certificados de los usuarios.
e) Establecer los mecanismos y procedimientos de seguridad de la información que permitan que los certificados digitales emitidos por la AC de PSC Codex sean considerados como confiables.
f) Implementar procesos de renovación de certificados que faciliten la interacción del usuario, ya sea directamente en las oficinas de PSC Codex o de forma remota, siempre en apego a la normativa y criterios aplicables.
g) Garantizar que el suscriptor es la única persona que conoce la contraseña de su certificado digital, la cual de ninguna manera se almacenará en bases de datos o ficheros de información.
h) Notificar a los suscriptores y partes interesadas en el servicio de emisión de certificados digitales los procesos a seguir en caso de presentarse o presumirse la vulneración de los datos de creación de firma de la Autoridad Certificadora de PSC Codex.

Responsabilidades de la AC

Adicionalmente a las obligaciones que enuncia PSC Codex como Prestador de Servicios de Certificación acreditado para la emisión de certificados digitales, a continuación, se dan a conocer las responsabilidades de la organización con respecto a la prestación del servicio:

a) Para la recolección y manejo de datos personales, PSC Codex implementará procedimientos que privilegien la seguridad de la información teniendo como enfoque principal la confidencialidad de la información.
b) Poner a disposición de los suscriptores y partes interesadas mecanismos y procedimientos de consulta que permitan verificar el estatus del certificado.
c) PSC Codex pondrá a disposición de sus suscriptores, dentro de su sitio electrónico, los procedimientos para realizar la renovación o revocación de un certificado digital, así como los requisitos particulares para cada proceso.
d) PSC Codex resguardará en sus bases de datos la información del certificado digital, así como el archivo *.cer del certificado digital del usuario, manteniendo y garantizando la integridad y seguridad de la información del usuario conforme

lo establecido en la Ley Federal De Protección de Datos Personales en Posesión de los Particulares y su Reglamento.

e) Entregar los archivos correspondientes al certificado digital en el dispositivo de almacenamiento USB tipo A proporcionado por el usuario.

Obligaciones de los suscriptores

Con la finalidad de mantener un esquema de confiabilidad en el servicio de emisión de certificados digitales por parte de la AC de PSC Codex, es necesario que los suscriptores y sujetos relacionados observen conductas que no pongan en riesgo la confianza que las partes interesadas depositan en la AC de PSC Codex como parte de sus transacciones.

En ese sentido, los suscriptores y sujetos relacionados del servicio de emisión de certificados digitales por la AC de PSC Codex tendrán las obligaciones siguientes:

- Cumplir totalmente con toda la información y los procedimientos requeridos en relación con la identificación y autenticación según la Política de Certificados, relacionados para la emisión de Certificados.
- Revisar el Certificado emitido y asegurarse de que toda la información descrita es completa y exacta.
- Las declaraciones efectuadas ante el Agente Certificador durante la solicitud de su Certificado son verdaderas.
- Garantizar que su certificado digital sea fiable:
    - Datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
    - Datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
    - Es posible detectar cualquier alteración de la firma electrónica hecha después del momento de la firma;
- Aceptación del contenido de la Política de Certificación y Declaración de Prácticas de Certificación.
- Aceptación de la carta de aceptación de certificado digital
- Actuar con diligencia para evitar la utilización no autorizada de sus datos de creación de la firma.

Responsabilidades de los suscriptores

Una vez que PSC Codex genera y entrega el certificado digital solicitado a sus suscriptores, estos últimos serán responsables del uso y manejo que se dé al certificado digital, así como de las acciones o transacciones que se lleven a cabo por medio de este. Al respecto, los suscriptores del servicio tendrán las responsabilidades siguientes:

- Notificar a la Autoridad Certificadora o al Agente Certificador en el caso de que el Certificado contenga cualquier inexactitud.

- El titular del certificado, genera en privado los datos de generación de firma electrónica (llave privada).
- Establecer frase de seguridad, crear, conservar y utilizar de forma correcta su par de claves de acuerdo a la normatividad vigente.
- Proteger y almacenar su clave de anulación, su clave privada y su Certificado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Solicitar de manera oportuna a la Autoridad Certificadora o al Agente Certificador la revocación de su Certificado en caso de sospechar o tener conocimiento de que su clave privada ha sido robada, extraviada, o sea conocida por terceros.
- Toda la información proporcionada es verdadera y confiable.
- El titular del certificado conoce las tarifas de la Autoridad Certificadora de como Prestador de Servicios de Certificación y autoriza a que le sean emitidos los cargos correspondientes a la prestación de servicios que reciba.

Obligaciones de las partes que confían

Las partes que confían en el servicio de emisión de certificados digitales por parte de la AC de PSC Codex tienen la obligación de conocer los términos y condiciones del servicio prestado, donde se establecen los preceptos generales del servicio y su funcionamiento.

Adicionalmente, PSC Codex establece que es obligación de las partes que confían desarrollar los mecanismos necesarios para poder acceder a los medios de consulta de información y de validación de certificados digitales que PSC Codex establece, tales como la Lista de Revocación de Certificados y el Protocolo de Validación en Línea del Estatus del Certificado.

Responsabilidades de las partes que confían

En aquellas acciones o transacciones que requieran del uso de los certificados digitales emitidos por PSC Codex será responsabilidad de las partes que confían ejecutar las siguientes acciones:

- Verificar la cadena de certificación presente en el certificado.
- Verificar que el certificado este correctamente firmado por la AC de PSC Codex.
- Consultar el servicio de OCSP, así como la CRL, de PSC Codex para validar que el certificado no se encuentre revocado.
- Verificar los usos permitidos que se establecen dentro del certificado.
- Observar que el certificado no haya sido emitido con un propósito específico y de ser así, validar que la acción que se está realizando corresponda con dicho propósito.
- Considerar las limitaciones que se establecen para el uso de los certificados digitales emitidos por PSC Codex.

Objetivos de seguridad de la información

PSC Codex como parte de la implementación del SGSI ha establecido diversos objetivos para la seguridad de la información de sus servicios los cuales están orientados a

garantizar a los suscriptores y partes interesadas que los servicios que proporciona PSC Codex son confiables y brindan certeza en el manejo de la información y los datos generados. Ahora bien, PSC Codex ha definido una serie de objetivos generales aplicables a la organización y sus sistemas, además de objetivos de seguridad específicos para los servicios acreditados como PSC.

Los objetivos generales de seguridad de la información de PSC Codex, aplicables a los servicios de emisión de certificados digitales, sellos digitales de tiempo y constancias de conservación de mensajes de datos, son los siguientes:

1. Mantener la Política de Seguridad de la Información de PSC Codex actualizada conforme a los riesgos y retos que representan los avances tecnológicos para asegurar su eficacia.
2. Generar lineamientos para la administración de la información generada por PSC Codex conforme a su nivel de criticidad asegurando el cumplimiento de las principales características de la seguridad de la información como son: integridad, disponibilidad, confidencialidad y no repudio.
3. Garantizar que los servicios que ofrece PSC Codex como Prestador de Servicios de Certificación se mantienen accesibles y disponibles para suscriptores y partes interesadas.
4. Gestionar la información que se recibe y genera como parte de los servicios que se tienen acreditados asegurando en todo momento la confidencialidad de la información.
5. Establecer procesos y mecanismos de verificación para garantizar que la información que se genera como resultado de los servicios se mantiene integra e inalterable en todas las fases de los servicios.
6. Implementar mecanismos de seguridad y autenticidad que permitan asegurar que los servicios acreditados como PSC únicamente se brindan a los suscriptores y partes interesadas que cumplan con los requerimientos que se establecen en las Políticas y Declaración de Prácticas de cada servicio.
7. Definir perímetros de control de acceso a las áreas seguras tanto de los centros de datos como de las oficinas administrativas para resguardar la información de los servicios que PSC Codex considera como información crítica.
8. Asegurar la protección de la infraestructura crítica, definida en el Análisis y Evaluación de Riesgos y Amenazas implementando correctamente los protocolos de seguridad que establecen los centros de datos contratados.
9. Configurar las redes internas de la infraestructura de los servicios de PSC Codex como PSC para que la comunicación se permita únicamente entre los equipos que componen la infraestructura.
10. Evitar la fuga de información generada como parte de los servicios de PSC Codex a partir de la concientización organizacional respecto de la importancia de cada uno de los colaboradores en la consecución de los objetivos.
11. Hay que asegurar que los certificados digitales son emitidos únicamente por los Agentes Certificadores acreditados ante la Secretaría de Economía.
12. Establecer de forma clara las obligaciones y responsabilidades que adquieren los suscriptores de los certificados digitales emitidos por PSC Codex.
13. Mantener disponible de forma permanente el protocolo de validación en línea de estatus de certificados u OCSP para la verificación del estatus de certificados por las partes interesadas.

14. Publicar la lista de revocación de certificados o CLR de forma permanente en periodos que no excedan el plazo de 24 horas.

Requerimientos de la práctica de la AC

La Autoridad Certificadora de PSC Codex está comprometida a garantizar que los procedimientos que forman parte de la emisión de certificados, es decir, todos aquellos relacionados con los servicio de certificación están alineados con los procesos de seguridad de la información que PSC Codex ha definido en documentos de seguridad como: Política de Seguridad de la Información, Plan de Seguridad de Sistemas, Sistema de Gestión de Seguridad de la Información, Planes de Continuidad y Análisis de Riesgos.

Al respecto, PSC Codex busca generar un equilibrio entre el proceso de implementación de controles de seguridad con los métodos que pueden ser empleados para la emisión de un certificado digital buscando minimizar las restricciones sobre los procesos de la Autoridad Certificadora.

PKI, ciclo de vida de los datos de creación de firma de la AC

Generación de las llaves de la Autoridad Certificadora

Para la generación del certificado de la Autoridad Certificadora de PSC Codex, la Ceremonia de Generación se realiza, conforme al apartado denominado "*Seguridad física y ambiental*" del presente documento, donde dicho apartado establece las medidas de seguridad física y ambientales que se deben de seguir durante la Ceremonia.

Atendiendo a las recomendaciones que se establecen, la Ceremonia de generación del certificado de la Autoridad Certificadora de PSC Codex se llevará a cabo en las instalaciones de los centros de datos principal y redundante que PSC Codex ha habilitado para la prestación del servicio y que alojan los módulos criptográficos. La ubicación de los centros de datos de PSC Codex, así como las medidas de seguridad física que los mimos establecen se encuentran descritas a detalle en la Política de Seguridad Física que se presentó a la Secretaría de Economía durante el proceso de acreditación.

En la Ceremonia de Generación de los datos de creación de firma de la Autoridad Certificadora de PSC Codex participa el personal asignado por la Secretaría de Economía, así como los elementos humanos que PSC Codex presentó para la acreditación de dicho servicio. Como parte de las medidas de seguridad que se toman durante la generación del certificado, todo el personal que ingresa a los centros deberá registrarse y su acceso estará autorizado por el Auxiliar de Apoyo Informático de Seguridad.

El certificado se generará y almacenará en un módulo criptográfico que cumple con los requisitos que establecen las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, es decir, es un módulo criptográfico

certificado en el estándar FIPS 140-2 nivel 3. También, en concordancia con la Regla 12 de las Reglas Generales, el certificado de la Autoridad Certificadora de PSC Codex tendrá una vigencia de hasta cuatro quintas partes del periodo de validez del Certificado de la Autoridad Certificadora de la Secretaría de Economía.

Tanto la longitud de llave, como el algoritmo mediante el cual se emite el certificado deberán ser los establecidos por la Secretaría de Economía y deberán ser reconocidos por el mercado con relación a procesos de infraestructuras PKI. En este caso la longitud de llave será de 4096 bits y se utilizará el algoritmo criptográfico conocido como SHA-256.

PSC Codex tendrá la responsabilidad de dar seguimiento a la fecha de vigencia del certificado de su Autoridad Certificadora y en un lapso no menor a dos años, respecto de la fecha de fin de vigencia, solicitará a la Secretaría de Economía la emisión de un nuevo certificado, el cual deberá ser generado y distribuido conforme se señala en el presente Plan de Administración de Claves.

PSC Codex se asegurará que el proceso de renovación del certificado de su Autoridad Certificadora, no se presentarán inconvenientes en la prestación del servicio que puedan afectar a las partes interesadas. Es factible que, al momento de presentar la solicitud de renovación del certificado de su Autoridad Certificadora, PSC Codex cuente con certificados de clientes que aun se encuentren vigentes, para ello, PSC Codex solicitará a la Secretaría de Economía mantener el certificado que se encuentra operativo con estatus de activo y vigente, comprometiéndose a no emitir nuevos certificados subordinados a este una vez que se emita el certificado que se solicita para la renovación.

Almacenamiento y protección de los datos de creación de firma

PSC Codex para la operación de su servicio de emisión de certificados digitales cuenta con dos módulos criptográficos nShield Connect XC para el almacenamiento, resguardo y protección de sus datos de creación de firma que, conforme a los requisitos que establecen las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación y el apartado 7.2.2 del framework de referencia, están certificados con el estándar FIPS 140-2 nivel 3. Estos módulos criptográficos se encuentran ubicados dentro de los centros de datos que alojan la infraestructura de Codex como PSC.

Para incrementar la seguridad de los datos de creación de firma de la Autoridad Certificadora aun y cuando los certificados se almacenan en el HSM, el acceso físico a dichos módulos se encuentra limitado únicamente al Profesional Informático y al Auxiliar de Apoyo Informático de Seguridad quienes son las únicas personas autorizadas para acceder a los racks donde se encuentran ubicados los equipos en los centros de datos.

Respaldo del certificado

El proceso de respaldo de los datos de creación de firma de la Autoridad Certificadora de PSC Codex se considera como un proceso de alta sensibilidad, pues por un lado

permitirá a la organización activar procesos de recuperación en caso de ser requerido; pero por otro lado requiere un minucioso control del proceso de respaldo y control de la cadena de custodia de los archivos generados.

Los responsables de llevar a cabo este proceso son el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad quienes ejecutaran el proceso de respaldo conforme a las indicaciones proporcionadas por el fabricante dentro de la documentación del equipo. Tratándose del primer respaldo del Security World y de los datos de creación de firma, el respaldo deberá considerar que los archivos y directorios derivados del respaldo del certificado deberán generarse cifrados y protegidos por contraseña, dentro de una unidad de almacenamiento extraíble destinada para ese fin. La contraseña del archivo cifrado se entrega en sobre cerrado al Profesional Jurídico quien deberá generar un acta de las actividades desarrolladas y posteriormente resguardar el dispositivo de respaldo y la contraseña.

Ahora bien, conforme a las recomendaciones que establece el fabricante con relación al respaldo de la información generada en el HSM y como parte del Security World, PSC Codex realiza copias de respaldo de forma quincenal de acuerdo con los procedimientos de respaldo de la información que se tienen definidos al interior de la organización. Es importante mencionar que la información que se genera como parte de los respaldos se considera segura y sin riesgo de poder ser aprovechada por terceros ya que los respaldos se encuentran cifrados utilizando las llaves de Seguridad del Security World.

Recuperación del certificado

El proceso de recuperación de los datos de creación de firma de la Autoridad Certificadora de PSC Codex hace uso de los archivos de respaldo, descritos en el apartado anterior, y conforme al procedimiento que establece el fabricante requiere de la implementación de un módulo criptográfico con las mismas características a aquel que fue utilizado para generar los archivos de respaldo.

Es importante mencionar que no basta con tener con un módulo criptográfico de las mismas características a aquel con el cual se generó el respaldo, sino que es necesario contar con los elementos de administración del Security World dentro del cual se generaron los certificados digitales. Para ello, es necesario que durante el proceso de recuperación de los datos de creación de firma los operadores del módulo, en el caso de PSC Codex el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, cuenten con las tarjetas de administración y operación correspondientes del Security World, así como con sus respectivas contraseñas.

Una vez que le personal a cargo se asegura contar con los elementos mencionados para iniciar el proceso de recuperación, es necesario cargar los archivos de respaldo en el directorio *"file system*" del dispositivo y utilizar las llaves de Seguridad del Security World para decifrar los archivos y poder iniciar el proceso de configuración y recuperación.

Cabe mencionar que, en caso de no contar con la llave de Seguridad del Security World o con las tarjetas de administración u operación requeridas conforme a la configuración del HSM no se podrá llevar a cabo el proceso de recuperación y se deberá considerar declarar el fin del ciclo de vida del módulo criptográfico.

Distribución de la llave pública

Los procesos y servicios basados en infraestructura de clave pública, como es el caso del servicio de emisión de certificados digitales de PSC Codex, tienen la obligación y el compromiso de asegurar que las partes interesadas puedan verificar la autenticidad e integridad de los procesos que de ella emanan.

Al respecto, PSC Codex distribuye la llave pública de su Autoridad Certificadora a las partes interesadas en su servicio de emisión de certificados digitales con la finalidad de que puedan verificar que la información contenida en el certificado de su Autoridad Certificadora coincide con los certificados que se emiten a sus clientes y, por tanto, es posible verificar y validar la cadena de certificación, estatus del certificados y validez de la autoridad que los emite.

El certificado se encuentra disponible en el portal de internet de PSC Codex, en la dirección electrónica https://www.psccodex.com/practicas_certificados/ así como en el portal de la Secretaría de Economía, en la dirección electrónica http://www.firmadigital.gob.mx/directorio.html donde además se podrá consultar la acreditación de PSC Codex, como Prestador de Servicios de Certificación, publicada en el Diario Oficial de la Federación.

Resguardo de claves privadas de los suscriptores

Siguiendo las recomendaciones que establece la Directiva de Firma Electrónica 1999/93/EC y dado que los certificados que emita a suscriptores y sujetos relacionados serán utilizados para procesos de firma electrónica avanzada, PSC Codex no resguardará las llaves privadas de los datos de creación de firma de sus usuarios, mismas que entregará al momento de la generación del certificado sin la posibilidad de obtenerlas nuevamente. En caso de que el usuario pierda el acceso a su llave privada será necesario realizar la revocación del certificado y solicitar la generación de uno nuevo.

Longitud de las claves

El certificado de la Autoridad Certificadora de PSC Codex se generará con una longitud mínima de 4096 bits y los certificados de los clientes o usuarios del servicio de emisión de certificados digitales de PSC Codex tendrán una longitud mínima de 2048 bits de conformidad con las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

Ahora bien, para la generación de los certificados, PSC Codex utilizará el algoritmo criptográfico de firmado que publica la Secretaría de Economía en la página http://www.firmadigital.gob.mx/marco_juridico.html. El algoritmo que actualmente se encuentra señalado en dicha página y, por tanto, será el utilizado por PSC Codex es el conocido como SHA-256.

La longitud de los certificados digitales, así como el algoritmo criptográfico utilizado, se ajustarán cuando los avances tecnológicos lo requieran y la Secretaría de Economía así lo comunique.

Algoritmo de firma electrónica avanzada

PSC Codex para garantizar un nivel adecuado de seguridad tanto para los certificados de los servicios que tiene acreditados como Prestador de Servicios de Certificación, así como para los certificados digitales que emite a sus clientes y suscriptores utiliza el algoritmo conocido como RSA el cual se encuentra definido dentro del estándar FIPS PUB 186-4. Este estándar define los procedimientos y características que se deben de considerar en la emisión de un par de llaves de firma electrónica para las cuales PSC Codex expresa su conformidad y apego.

Uso del certificado

Una vez que la Secretaría de Economía otorga la acreditación a PSC Codex como PSC para el servicio de emisión de Certificados Digitales, se emiten un par de llaves con los datos de creación de firma de uso específico del servicio. Es decir, el certificado de la Autoridad Certificadora de PSC Codex únicamente será utilizado por PSC Codex para la emisión de certificados digitales subordinados a su Autoridad Certificadora a solicitud de los suscriptores y sujetos relacionados de este servicio.

PSC Codex con la finalidad de evitar que el certificado de su Autoridad Certificadora sea utilizado para propósitos diferentes para los que fue previsto resguardara el certificado conforme se señala en el apartado de “Gestión del certificado” del presente documento.

Fin del ciclo de vida del certificado

Se dice que el certificado de la Autoridad Certificadora ha llegado al final de su ciclo de vida cuando se cumplen algunas condiciones que impiden que dicha autoridad pueda seguir garantizando la integridad y confidencialidad de la información que se genera en los procesos que utilizan dicho certificado o cuando se alcanza el tiempo de vigencia que se señala durante la ceremonia de generación de los datos de creación de firma.

Los supuestos que pueden derivar en el final del ciclo de vida son los siguientes:

1. Fin de vigencia. Cuando se ha alcanzado la fecha señalada como de término de vigencia del certificado de la Autoridad Certificadora de acuerdo con las consideraciones efectuadas durante la ceremonia de generación de llaves.
2. Revocación de claves. Cuando PSC Codex determine que no se cumplen las condiciones de seguridad del certificado de su Autoridad Certificadora y por tanto no es posible continuar garantizando la integridad de la información. Entre los supuestos que pueden originar la solicitud de revocación se encuentran: vulneración de las claves de la Autoridad Certificadora, pérdida de la frase de seguridad del par de llaves, fin del ciclo de vida del módulo criptográfico, entre otros.

3. Función hash obsoleta. Cuando la función hash que se genera a partir del algoritmo criptográfico autorizado por la Secretaría de Economía se considere vulnerable u obsoleta y la propia Secretaría emita los nuevos lineamientos de aplicación de algoritmo criptográfico y función hash.
4. Longitud de claves no segura. Cuando la longitud de las claves no se considere suficiente para garantizar la integridad de la información y la Secretaría de Economía emita nuevos lineamientos respecto a la longitud que debe de ser utilizada para la emisión de los certificados de la Autoridad Certificadora.

Para cada uno de estos supuestos PSC Codex mantendrá una estrecha y continua comunicación con la Secretaría de Economía, con la finalidad de solicitar la emisión de un nuevo par de llaves para poder continuar prestando el servicio de emisión de certificados digitales, conforme a los supuestos y requisitos aplicables en cada escenario.

En el supuesto en el que se solicita la revocación del certificado por la pérdida de confianza de los datos de creación de firma o por la sospecha de la vulneración de estos, PSC Codex procederá a revocar de forma inmediata todos aquellos certificados digitales emitidos con el certificado que se considera comprometido. Una vez revocados los certificados establecerá comunicación con los clientes afectados, así como con las partes interesadas, para dar a conocer el proceso de emisión de nuevos certificados una vez que la Secretaría de Economía entregue los nuevos datos de creación de firma para la Autoridad Certificadora.

Ciclo de vida de los módulos criptográficos

Los servicios de certificación tienen como uno de sus principales activos críticos al módulo criptográfico esto ya que, como se ha venido señalando, es el dispositivo que resguarda los datos de creación de firma de la Autoridad Certificadora de PSC Codex como Prestador de Servicios de Certificación para el servicio de emisión de certificados digitales, es decir, es el centro y origen de la confianza del servicio.

En ese sentido, PSC Codex ha establecido una serie de medidas y controles que permiten garantizar la seguridad de sus módulos criptográficos y, por ende, de sus Datos de Creación de Firma Electrónica Avanzada.

El detalle del ciclo de vida de los módulos criptográficos de la Autoridad Certificadora de PSC Codex puede consultarse en el documento denominado "*Plan de Administración de Claves de la AC*".

Destrucción de la llave privada de la Autoridad Certificadora

PSC Codex, atendiendo a los procedimientos de seguridad organizacionales, una vez que se alcanza el fin del ciclo de vida del certificado de la Autoridad Certificadora a través del Profesional Informático y del Auxiliar de Apoyo Informático de Seguridad procederá a la destrucción o eliminación de la llave privada del certificado que se encuentra resguardada dentro del módulo criptográfico. Este procedimiento se llevará a

cabo haciendo uso de las herramientas que el propio módulo criptográfico proporcione para la eliminación segura de las llaves privadas.

La llave pública del certificado de la Autoridad Certificadora será resguardada por PSC Codex y podrá ser puesta a disposición de las partes interesadas cuando las mismas requieran ejecutar procesos de verificación. La distribución de la llave pública se llevará a cabo en los medios electrónicos que permitan garantizar su integridad y el procedimiento para obtener la llave será publicado en la página de PSC Codex cuando el supuesto se presente.

PKI, ciclo de vida de los certificados

El ciclo de vida de los certificados digitales que PSC Codex emite a sus suscriptores y sujetos relacionados contempla todas aquellas actividades y procesos que se ejecutan desde que el usuario registra su información hasta el momento en que el certificado deja de ser válido, lo cual puede resultar como consecuencia de la revocación del certificado o por el fin del periodo de vigencia establecido en el momento de la generación.

Proceso de emisión de un certificado digital

Para la emisión de un certificado digital los suscriptores y/o sujetos relacionados deben completar las etapas que se han definido para la emisión del certificado las cuales tiene como objetivo recabar y verificar la información que se contendrá dentro de la llave pública del titular y que le servirá como medio de identificación en los medios electrónicos en los que actué.

En general, la emisión de un certificado digital requiere que se de cumplimiento a los procesos operativos relacionados con el registro de información del solicitante, la verificación de identidad y la generación del certificado, mismos procedimientos que se describen en los apartados siguientes.

Registro de información del solicitante

El proceso emisión de un certificado es considerado por PSC Codex como un trámite personal que debe ser realizado directamente por el interesado en función de los alcances y obligaciones que conlleva la emisión y uso de un certificado digital. Por ello, PSC Codex dentro de su sitio electrónico de alta disponibilidad, relacionado con su Autoridad Registradora, permite a los interesados realizar el registro y generar un perfil de usuario, por lo cual deben aceptar el Aviso de Privacidad y los términos y condiciones de la plataforma en dicho entorno digital, en el cual les es asignado un usuario y contraseña con el cual pueden ingresar a la plataforma y realizar diversas acciones, entre las que se encuentra el registro de información como parte de la solicitud de un certificado digital. Lo anterior resulta relevante ya que permite asegurar que el registro de información se realiza de forma personal y brinda herramientas o datos adicionales a PSC Codex para garantizar que los Datos de Creación de Firma Electrónica son capturados directamente por el interesado.

En la captura de información para la generación del requerimiento de emisión de un certificado digital, PSC Codex atendiendo al principio de proporcionalidad que establecen la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y su Reglamento, únicamente recopila los datos que resultan fundamentales para la emisión de dicho certificado. Para ello, considera como base de información los atributos señalados dentro de las Disposiciones Generales de la Ley de Firma Electrónica Avanzada para la emisión de certificados digitales.

Es importante mencionar que la captura de información y la generación del requerimiento no implica la emisión de un certificado digital, lo cual estará sujeto al proceso de verificación de identidad que realizará PSC Codex para asegurar la identidad del solicitante. En caso de que no se lleve a cabo la emisión del certificado debido a que no se pudo realizar la verificación fehaciente de la identidad del solicitante, el usuario no se presentó a la cita de emisión del certificado, el usuario no concluyó el proceso, no requirió del certificado o cualquier otra circunstancia que no permita emitir el certificado digital los datos personales del usuario serán resguardados por PSC Codex bajo los mismos mecanismos de seguridad incluyendo Políticas, procesos y mecanismos aplicables a los datos de aquellos usuarios que si culminaron el proceso. Resulta relevante destacar que la información de aquellos usuarios que no hayan completado el proceso de emisión del certificado será eliminada de la base de datos de PSC Codex una vez que transcurra el plazo de setenta y dos meses contados a partir del último movimiento del usuario en el sistema.

Como parte del proceso de registro de información, las personas físicas que soliciten un certificado digital deberán ingresar la información siguiente:

1. Nombre
2. Apellido Paterno
3. Apellido Materno
4. Fecha de Nacimiento
5. Correo electrónico
6. Registro Federal de Contribuyentes
7. Clave Única de Registro de Población
8. Número Telefónico
9. Archivo electrónico de su documento de identidad (Credencial de elector/INE/IFE, Pasaporte, Cédula Profesional con fotografía)
10. Archivo electrónico del comprobante de domicilio
11. Archivo electrónico de su acta de nacimiento o carta de naturalización en caso de ser mexicano
12. Archivo electrónico de su documento migratorio FM2
13. Domicilio para recibir notificaciones

En caso de que la solicitud de emisión del certificado digital sea generada por un sujeto relacionado, se deberá de ingresar la información señalada para los certificados emitidos a una persona física, además de la información siguiente:

1. Registro Federal de Contribuyentes de la sociedad que solicita la emisión del certificado.
2. Carta de solicitud de emisión del certificado, en hoja membretada firmada por el representante legal de la sociedad.

Una vez que concluye el proceso de registro, el solicitante deberá dentro de la propia plataforma de registro, deberá agendar una cita con el agente certificador para presentarse en las oficinas de PSC Codex a concluir el proceso de emisión del certificado digital y donde se llevará a cabo el proceso de verificación de identidad.

Los datos registrados dentro de la plataforma, conforme se señala en el Aviso de Privacidad presentado al usuario tendrán como finalidad la emisión de un certificado digital y serán resguardados tal cual son ingresados por el usuario dentro de la base de datos de información de PSC Codex.

La transferencia de datos entre la Autoridad Registradora y la Autoridad Certificadora se llevará a cabo a través de medios de comunicación seguros privilegiando aquellos que puedan ser cifrados haciendo uso de las tecnologías disponibles.

Los datos recabados estarán sujetos a los procedimientos y políticas de seguridad que se mencionan en el apartado de protección de datos del presente documento.

Verificación de identidad

PSC Codex como Prestador de Servicios de Certificación acreditado para el servicio de emisión de certificados digitales a través de su Autoridad Certificadora y Registradora, debe realizar un proceso de verificación de la identidad de los suscriptores y partes interesadas que soliciten la emisión de un certificado digital. Como parte de este proceso PSC Codex debe de garantizar fehacientemente la identidad del solicitante, con lo cual se dará certeza a las transacciones que se realicen haciendo uso del certificado digital emitido.

El proceso de verificación de identidad que implementa PSC, requiere que el solicitante integre como parte del requerimiento de emisión de certificado diversos documentos, entre los que destaca la identificación oficial con fotografía. Una vez que el solicitante se presenta en las oficinas de PSC Codex, la primera validación de sus documentos será realizada por el personal de Atención a Clientes, según el procedimiento "*Autenticar Identidad del Usuario"*, posteriormente con el Agente Certificador, quien cotejará la información que se capturó en el sistema de requerimientos, contra la información contenida en la identificación y demás documentos que debe de presentar en original el interesado para su cotejo.

Como parte del proceso de verificación de identidad PSC Codex hará uso de las diversas plataformas que ponen a disposición las autoridades para la verificación de la información asociada a la identidad de las personas, como son las siguientes:

- Credencial de elector. https://listanominal.ine.mx/scpln/
- Cédula profesional. https://www.cedulaprofesional.sep.gob.mx/cedula/presidencia/indexAvanzada.action
- CURP. https://www.gob.mx/curp/
- RFC. https://agsc.siat.sat.gob.mx/PTSC/ValidaRFC/index.jsf

El detalle del proceso de verificación de identidad y documental para personas físicas se puede consultar en el documento "*Autenticar Identidad del Usuario"*.

Generación del certificado

PCS Codex como Autoridad Certificadora acreditada por la Secretaría de Economía, ha establecido los medios y procesos necesarios que le permiten asegurar que los certificados digitales que emite a suscriptores y sujetos relacionados se generan bajo estrictos controles de seguridad a nivel de hardware y software, que le permiten garantizar la autenticidad de dichos certificados.

Es importante resaltar que los certificados digitales que emite PSC Codex únicamente podrán ser generados por el o los Agentes Certificadores que se han acreditado ante la Secretaría de Economía y que son los responsables de realizar el proceso de emisión. Los certificados digitales solamente podrán ser emitidos una vez que el agente certificador ha ejecutado por completo y de manera satisfactoria el proceso de verificación de la identidad del suscriptor o sujeto relacionado que solicita el certificado digital.

Además, al concluir el proceso de emisión del certificado se proporcionará al interesado una serie de documentos que tienen como finalidad que el usuario exprese su voluntad de dar cumplimiento a las obligaciones señaladas en el presente documento, así como en los términos y condiciones del servicio; además de que deberá firmar el aviso de privacidad de PSC Codex que se emite en cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento.

Antes, durante y después del proceso de emisión del certificado PSC Codex ha implementado diversos mecanismos que lo ayudan a proteger la confidencialidad e integridad de la información que se recaba como parte del proceso de registro y emisión del certificado digital en atención a lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

El detalle del proceso de generación de un certificado tanto para personas físicas se puede consultar en los documentos "*Proceso para Solicitar un Requerimiento para emitir un Certificado Digital*" y "*Emitir Certificado Digital"*.

Estructura de los certificados emitidos por la AC de PSC Codex

Los certificados que son emitidos por la AC de PSC Codex se emiten de conformidad con el Rfc 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" el cual indica los campos y requisitos que deben de cumplir los certificados emitidos por una AC. Entre las características más importantes de los certificados emitidos por la AC de PSC Codex, se encuentran:

1. Los certificados son emitidos conforme la versión 3 del X.509, al contener un identificador único y hacer uso de extensiones.
2. El número de serie es un número entero no negativo, el cual tiene una longitud máxima de ocho octetos.
3. El periodo de validez de los certificados se expresa en una secuencia de dos fechas las cuales indican el inicio y fin de la vigencia. En el caso de los

certificados de la AC de PSC Codex dichas fechas se expresarán en tiempo UTC conforme se señala en el apartado 4.1.2.5.1 del Rfc 5280.

Ahora bien, para que los certificados que emite la AC de PSC Codex sean considerados válidos, estos contendrán al menos los siguientes datos:

1. La indicación de que se expiden como tales.
2. Identificador único del certificado.
3. La identificación del Prestador de Servicios de Certificación que expide el Certificado, razón social, su nombre de dominio de Internet, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría.
4. Nombre del titular del Certificado;
5. Periodo de vigencia del Certificado;
6. Fecha y hora de la emisión del Certificado;
7. El alcance de las responsabilidades que asume el Prestador de Servicios de Certificación, y
8. La referencia de la tecnología empleada para la creación de la Firma Electrónica.

Extensiones que se incluyen en los certificados

Los certificados emitidos por la AC de PSC Codex al ser generados bajo el estándar X.509 v3 deben hacer uso de extensiones las cuales ayudan a proporcionar métodos para asociar atributos adicionales a los certificados digitales y definir algunas características relevantes para su uso.

A continuación, se describen las extensiones más importantes utilizadas en la emisión de los certificados por la AC de PSC Codex.

Identificador de clave de autoridad.

Este atributo proporciona los medios para identificar la llave pública correspondiente a la llave privada que fue utilizada para firmar el certificado emitido. La identificación se basa en la clave de identificación del certificado que firma, en el nombre del emisor o en el número de serie.

Usos permitidos del certificado digital (Alcance del certificado)

Este atributo señala el propósito o alcance para el cual fue emitido un certificado digital, así como el uso permitido que tendrá el certificado. En la emisión del certificado digital se pueden señalar los siguientes propósitos:

1. Firma digital
2. No repudio
3. Cifrado de llaves
4. Cifrado de información
5. Firma de llaves de certificado
6. Firma de CRL
7. Solo cifrado
8. Solo descifrado

Políticas de certificación

Indica el Objeto Identificador (OID) que fue asignado por la Secretaría de Economía a las Políticas de Certificación de PSC Codex una vez que emitió su acreditación como Prestador de Servicios de Certificación.

Restricciones básicas

La extensión de restricciones básicas identifica si el certificado pertenece a una Autoridad Certificadora y la profundidad de esta dentro de una cadena de certificación. Es decir, el número de AC's de certificados que se habrán de validar en la cadena de certificación para garantizar la validez del certificado.

Propósito específico

Esta extensión permite a las organizaciones que requieren de la emisión de certificados digitales señalar uno o más propósitos para los cuales podrá ser utilizado el certificado, en adición a los usos básicos permitidos señalados en la extensión correspondiente.

En caso de requerirse la emisión de certificados de propósito específico, estos se deberán de incluir de conformidad con las recomendaciones que establece el X.660.

Punto de distribución de CRL

Indica los mecanismos o rutas a través de las cuales los suscriptores o partes interesadas en los certificados emitidos por la AC de PSC Codex pueden obtener la información de la Lista de Revocación de Certificados. En el caso de la CRL de PSC Codex, la CRL se pondrá a disposición a través del protocolo HTTPS indicando dentro del certificado la URI con la cual se podrá acceder a la lista.

Acceso a la información de la autoridad

Esta extensión indica la forma en que los suscriptores y partes interesadas en el uso de certificados digitales pueden obtener información respecto de la AC que los emite, en este caso de la AC de PSC Codex. En el caso de PSC Codex, esta extensión es utilizada en la emisión de certificados para indicar la ruta de acceso al OCSP de su AC.

Alcance de los certificados emitidos

PSC Codex durante el proceso de generación de los certificados digitales brindará la información correspondiente a sus suscriptores respecto de los alcances que tienen los certificados digitales emitidos por su AC. Una vez que se hace de conocimiento de los suscriptores, PSC Codex hará uso de la extensión correspondiente a los "Usos permitidos del certificado digital" para señalar las acciones para las cuales será válido el certificado emitido.

Los certificados digitales emitidos por la AC de PSC Codex podrán tener los alcances siguientes:

1. Firma digital
2. No repudio
3. Cifrado de llaves
4. Cifrado de información

5. Firma de llaves de certificado
6. Firma de CRL
7. Solo cifrado
8. Solo descifrado

Aceptación del certificado

Una vez que el certificado fue emitido satisfactoriamente, el solicitante deberá dar su aceptación expresa respecto de la emisión del certificado donde exprese su conformidad con la recepción del certificado que se emite, así como de la información contenida en el mismo. El agente certificador, a su vez, hará del conocimiento del titular del certificado los objetivos, alcances y limitaciones del certificado, así como de las obligaciones y responsabilidades que contrae el titular del certificado como parte del proceso de emisión y uso.

La información será proporcionada por el agente certificador de forma oral y escrita, debiendo el titular del certificado firmar un tanto de la información a través del cual expresará su conocimiento y consentimiento respecto del alcance, obligaciones y responsabilidades derivadas del uso del certificado. En caso de que el titular se rehúse a firmar la documentación señalada, PSC Codex se reserva el derecho a revocar el certificado.

Vigencia del certificado

Los certificados digitales emitidos por la Autoridad Certificadora de PSC Codex tendrán una vigencia de hasta dos años contados a partir de la fecha de generación del certificado, de conformidad con el artículo 109 fracción del Código de Comercio. Si a petición de los suscriptores se requiriera que el tiempo de vigencia fuera menor, PSC Codex podrá emitir dichos certificados conforme la petición y acuerdo que se tenga con el suscriptor, teniendo como periodo mínimo de vigencia un año.

En ninguna circunstancia PSC Codex, ni sus agentes certificadores emitirán certificados digitales con un periodo de vigencia mayor a dos años.

Modificación del certificado

Los procesos de operación de la AC de PSC Codex no contemplan la posibilidad de realizar la modificación de los certificados digitales. Si por algún motivo el titular del certificado requiere de la modificación de alguno de los datos que se incluyen en el certificado, deberá atender a los procedimientos y requerimientos descritos en el apartado “*Revocación presencial*” del presente documento.

Renovación del certificado

Los certificados digitales emitidos por PSC Codex tienen establecido un periodo de vigencia el cual se define durante el proceso de emisión del certificado y conforme al acuerdo contractual que tenga PSC Codex con los suscriptores, pudiendo emitirse los

certificados con un tiempo de vigencia menor o igual a dos años. Una vez que se alcance la fecha de fin de vigencia o con una anterioridad máxima de un mes, los interesados podrán solicitar a PSC Codex la renovación de su certificado digital.

El proceso de renovación de los certificados de PSC Codex podrá realizarse de forma presencial o remota atendiendo a las características, especificaciones y limitantes para cada uno de estos procesos y siempre atendiendo a la limitante que establece la fracción VII de la Regla 63 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación que establece que la renovación de un certificado podrá llevarse a cabo de manera alterna y remota, siempre y cuando el certificado se encuentre vigente y en ningún caso podrá renovarse un certificado de manera remota en dos ocasiones consecutivas.

Renovación presencial

El proceso de renovación presencial requiere que el suscriptor o sujeto relacionado complete los procesos descritos en los apartados denominados "Registro de información del solicitante" y "Generación del certificado" del presente documento. Como parte de este proceso se deberá verificar la identidad del solicitante conforme se señala en el apartado de "*Verificación de identidad*" debiendo el usuario presentar la documentación solicitada durante el proceso de registro para el cotejo por parte del agente certificador.

El detalle del proceso de renovación remota de un certificado digital puede consultarse en el documento *"Renovar Certificado Digital".*

Renovación remota

PSC Codex conforme lo establece la fracción VII de la Regla 63 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación tiene implementada, dentro de su plataforma de emisión de certificados, la funcionalidad de renovar los certificados digitales de sus suscriptores y sujetos relacionados de forma remota.

Para poder realizar la renovación de forma remota se deberán de cumplir los requisitos siguientes:

1. El certificado digital del suscriptor o sujeto relacionado deberá encontrarse vigente.
2. El titular del certificado a renovar deberá contar con la llave pública, llave privada y contraseña del certificado que se va a renovar.
3. El certificado digital que se renovará deberá haberse emitido o renovado de manera presencial en compañía del agente certificador de PSC Codex.
4. Los datos de identificación del suscriptor o sujeto relacionado que integrarán el certificado por emitirse serán los datos que se incluyen en el certificado que se desea renovar.
5. En ninguna circunstancia se podrá realizar la renovación remota de un certificado digital en ocasiones consecutivas.

El proceso de renovación remota de un certificado digital emitido por PSC Codex realiza el proceso de verificación de la identidad del usuario a través del certificado digital que se desea renovar. Lo anterior considerando que el certificado digital se considera un

elemento de identidad que está relacionado con la identidad del usuario la cual fue verificada y/o registrada durante el proceso de generación del certificado.

Además, se considera que el certificado digital representa un proceso de autenticación de dos factores que requiere algo que posee el usuario y algo que el usuario sabe. En este caso, el usuario posee la llave pública y la llave privada del certificado digital y sabe la contraseña de dicho par de llaves, lo cual se fortalece con las cláusulas que se establecen en las obligaciones y responsabilidades que fueron del conocimiento del usuario al momento de generar su certificado digital, las cuales establecen que el usuario es responsable de resguardar su par de llaves y contraseña y evitar compartirlo con terceras personas.

Como parte del proceso de renovación del certificado el suscriptor deberá conocer y aceptar los términos y condiciones de uso del certificado emitido por PSC Codex a través de la plataforma que ha sido destinada para este efecto. Para ello, se presentará al usuario la información que permita dejar constancia de que el usuario conoce la información relativa a los alcances, limitaciones, obligaciones, responsabilidades derivadas de la renovación y utilización del certificado digital.

Para garantizar que el usuario conoce y acepta la información relativa a los alcances, limitaciones, obligaciones, responsabilidades derivadas de la renovación y utilización del certificado digital, PSC Codex habilitará una casilla de aceptación a través de la cual el usuario manifestará su conformidad con información presentada no siendo posible continuar el proceso si el usuario no manifiesta su aceptación marcando la casilla de verificación.

El detalle del proceso de renovación remota de un certificado digital puede consultarse en el documento "*Renovar Certificado Digital"*.

Distribución de los términos y condiciones

PSC Codex hace del conocimiento de sus suscriptores y sujetos relacionados, los términos y condiciones que son aplicables al servicio de emisión de Certificados Digitales que tiene acreditado como Prestador de Servicios de Certificación. Para ello, durante el proceso de registro de la solicitud de emisión del certificado digital solicita que el usuario indique que esta de acuerdo con los términos y condiciones del servicio. Además, durante el proceso de generación del certificado, el suscriptor o sujeto relacionado debe de firmar un documento en el cual expresa que esta de acuerdo y acepta los términos y condiciones del servicio; finalmente, PSC Codex como parte del proceso de entrega del certificado entrega una copia digital de la versión de los términos y condiciones que fue aceptada por el usuario.

Los términos y condiciones del servicio de emisión de Certificados Digitales de la Autoridad Certificadora de PSC Codex, entre otras cosas, contienen los puntos siguientes:

1. OID de la política aplicable.
2. Limitaciones del uso de los certificados.
3. Obligaciones y responsabilidades de los suscriptores.
4. Información del proceso de validación del certificado.

5. Sistema legal aplicable para la resolución de disputas y conflictos.

Notificación de la emisión del certificado a la SE

En cumplimiento a lo dispuesto en la Regla 76 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación y conforme al procedimiento establecido en el artículo 16o. del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación, PSC Codex remitirá, en tiempo real, una copia de los certificados emitidos por su Autoridad Certificadora a la Secretaría de Economía a través de los procedimientos definidos por esta Autoridad.

Ahora bien, cuando la Autoridad Certificadora de PSC Codex por caso fortuito o de fuerza mayor relacionado con la organización o con la Secretaría de Economía, no pueda remitir en tiempo real los certificados a través del procedimiento establecido, el personal de PSC Codex remitirá diariamente con posterioridad al cierre de operaciones (18:00 horas) vía correo electrónico la copia de los certificados emitidos durante ese día laboral.

En cualquiera de los casos señalados, el envío de los certificados se realizará mediante un archivo comprimido en formato ZIP cifrado por contraseña la cual será previamente proporcionada a la Secretaría de Economía solicitando el acuse de recibo correspondiente a fin de tener la certeza de que la información fue entregada en tiempo y forma.

Registro de los movimientos de un certificado

PSC Codex tiene la obligación de ejecutar procedimientos que permitan llevar un registro confiable de la fecha y hora en que se realiza cualquier acción relacionada con los certificados digitales que emite su Autoridad Certificadora, principalmente para la emisión y revocación de certificados.

En ese sentido, el proceso de registro de PSC Codex consiste en solicitar la emisión de un Sello Digital de Tiempo, a su Autoridad de Sellado Digital de Tiempo, para la emisión de cada uno de los certificados digitales que emite; mismo procedimiento se aplica cuando se realiza la revocación de un certificado digital por parte de los interesados. Un medio alternativo para obtener los sellos digitales de tiempo requeridos para la operación del servicio de emisión de certificados digitales, en caso de que el servicio de Sellos Digitales de Tiempo de PSC Codex no se encuentre disponible o que no se cuente con el servicio propio, es el consumo del servicio de emisión de Sellos Digitales de Tiempo a un PSC previamente acreditado por la Secretaría de Economía.

Los Sellos Digitales de Tiempo son almacenados en la base de datos de la Autoridad Certificadora de PSC Codex y se respaldan en el sistema de archivos de la propia Autoridad, permitiendo identificar el movimiento para el cual se emitió el Sello Digital.

Para la emisión del Sello Digital de Tiempo relacionado con la emisión del certificado digital, el mismo se generará obteniendo el hash de la llave pública del certificado indicando que se emite el sello digital como parte de la emisión de un certificado.

Revocación del certificado

Como parte del ciclo de vida de un certificado digital existen circunstancias que puedan derivar en la necesidad de revocar el certificado, es decir, ejecutar el proceso necesario para que el certificado digital pierda validez y no pueda ser utilizado para actuar con terceros. El proceso de revocación requiere que las partes interesadas en el certificado realicen el procedimiento a través de medios remotos o de la presentación de un escrito libre dirigido a PSC Codex.

Es importante recalcar que una vez que un certificado digital ha sido revocado, el mismo no podrá volver a ser habilitado y el interesado deberá iniciar el proceso de registro para la emisión de un nuevo certificado digital.

Motivos de revocación

PSC Codex como parte del proceso de generación del certificado hace de conocimiento de los suscriptores y sujetos relacionados los motivos que pueden derivar en la revocación de un certificado digital. Los motivos que se han establecido contemplan situaciones personales, sociales y de seguridad.

A continuación, se enlistan los motivos válidos para la solicitud de revocación de un certificado digital:

1. Incapacidad jurídica.
2. Revocación de poderes.
3. Deceso.
4. Retiro voluntario / involuntario de una empresa.
5. A petición de una Autoridad.
6. Extravío de la llave privada, olvido de la contraseña o indicios de que fueron comprometidas.
7. Cambio de nombre o cambio de denominación o razón social
8. Cambio de RFC
9. Cambio de Clave Única de Registro de Población
10. Error en la información del certificado una vez emitido

Revocación remota

PSC Codex para facilitar el proceso de revocación de un certificado, dentro del portal de usuarios registrados pone a disposición de los suscriptores y sujetos relacionados la herramienta de revocación remota con la cual podrán solicitar la revocación inmediata de un certificado.

Para poder hacer uso de esta herramienta, el interesado en realizar la revocación del certificado deberá ingresar a su perfil de usuario con sus credenciales de la plataforma y seleccionar el certificado digital que se desea revocar, además de contar con la contraseña de anulación, la cual se generó y registró durante el proceso de registro de solicitud del certificado.

Este proceso únicamente puede ser realizado por suscriptor o sujeto relacionado que cuente con la clave de anulación y una vez que concluye el proceso se generará el

comprobante de revocación en el cual se indican los datos generales del certificado que esta siendo revocado, así como el motivo de revocación seleccionado.

Al utilizar este medio de revocación, el certificado queda automáticamente revocado y su estatus se replicará de inmediato en el servicio de validación en línea OCSP.

Revocación vía escrito de solicitud

En caso de no contar con la clave de anulación, número de serie del certificado o RFC el suscriptor o sujeto relacionado deberá, mediante escrito libre, ingresar una solicitud de revocación certificado en medios impresos en las oficinas administrativas de PSC Codex. Una vez recibido el escrito de solicitud el agente certificador de PSC Codex acreditado ante la Secretaría de Economía, en compañía del solicitante realizará el proceso de revocación.

Para que el agente certificador de PSC Codex pueda iniciar el proceso de revocación del certificado, el solicitante o interesado deberá presentar la documentación siguiente:

a. Solicitud de revocación debidamente llenada y firmada.
b. Documento que demuestre la titularidad o propiedad del certificado, parentesco.
c. Identificación oficial del solicitante.
d. Documentos que acrediten las facultades de representación del solicitante.

A continuación, se relacionan los motivos de revocación de un certificado digital con las partes interesadas que pueden llevar a cabo el proceso de revocación.

Motivo	Documentación adicional	¿Quién puede realizar el proceso?
Incapacidad jurídica.	Copia certificada de sentencia, emitida por autoridad competente, de la declaración de la incapacidad de la persona y designación del tutor.	Persona que fue designada como tutor Acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización)
Revocación de poderes.	Protocolo notarial en el cual se hace constar la revocación de poderes del representante legal, así como el nombramiento u otorgamiento de nuevas facultades.	N/A
Deceso.	Acta de defunción. Documento de identidad que acredite el parentesco del solicitante con la persona fallecida. Permiso especial en caso de que no exista familia cercana.	Padre, madre, Hijos, Hermanos, Cónyuge del titular del certificado.
Retiro voluntario / involuntario de una empresa.	Carta de renuncia firmada. Baja del padrón de trabajadores del IMSS.	Patrón acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización) y documento que acredite la relación laboral
A petición de una Autoridad.	Documento judicial, federal, estatal, bancario, financiero donde conste la solicitud de la autoridad.	N/A
Extravío de la llave privada, olvido de la contraseña o indicios de que fueron comprometidas.	N/A	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización)
Cambio de nombre	Resolución judicial por el procedimiento de rectificación de acta de nacimiento, pre acta, nueva acta de nacimiento y anterior.	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización)

Motivo	Documentación adicional	¿Quién puede realizar el proceso?
Cambio de RFC	Acuse de actualización de situación fiscal. Nuevo RFC. RFC anterior.	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización).
Cambio de Clave Única de Registro de Población	Solicitud de corrección de datos de la CURP. Nueva CURP. CURP anterior.	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización).
Error en la información del certificado una vez emitido	N/A	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización).

Tabla 1 Requisitos para la solicitud de revocación de un certificado

PSC Codex establece un plazo máximo de 24 horas a partir de que se inicia el trámite de revocación para realizar la actualización de estatus del certificado, una vez concluido el proceso de revocación, el titular de dicho certificado será notificado respecto de la revocación a través del correo electrónico que se proporcionó como parte del procedo de generación del certificado digital.

Actualización de estatus del certificado

PSC Codex cuenta con dos procesos que permiten a los interesados conocer el estatus que tiene un certificado digital en relación con la Autoridad Certificadora que lo emite. Estos procesos de validación pueden realizarse utilizando el protocolo OCSP o descargando y consultando la CLR de la AC de PSC Codex.

En el caso de la revocación de un certificado emitido por PSC Codex, las partes interesadas podrán validar en tiempo real el estatus del certificado a través del protocolo de OCSP el cual esta disponible 24 horas los 365 días del año. Por otra parte, PSC Codex cuenta con un medio alterno de consulta que son las listas de revocación de certificados donde PSC Codex incluye la información referente a los certificados que ha emitido y que han sido revocados. La CRL de la AC de PSC Codex se publicará cada 24 horas a fin de que los interesados puedan contar con información actualizada.

La dirección donde se puede consultar el protocolo OCSP es:
https://www.app.psccodex.com/ocsp

La dirección de consulta de la CRL de PSC Codex es: www.app.psccodex.com/crl.

Administración y operación de la AC

Agentes Certificadores

Los Prestadores de Servicios de Certificación conforme a su normativa aplicable pueden habilitar a una o más personas físicas o morales como Agentes Certificadores quienes serán los encargados de verificar la identidad de los solicitantes del servicio de emisión de certificados digitales de acuerdo con lo establecido en la fracción I del artículo 104 del Código de Comercio que a la letra indica:

"Artículo 104. …

"I. Comprobar por sí o por medio de una persona física o moral que actúe en nombre y por cuenta suyos, la identidad de los solicitantes y cualesquiera circunstancias pertinentes para la emisión de los Certificados, utilizando cualquiera de los medios admitidos en derecho, siempre y cuando sean previamente notificados al solicitante. …"

En ese sentido, PSC Codex contempla que los interesados en fungir como Agente Certificador deberán entregar la solicitud correspondiente junto con la documentación, en original y copia, que a continuación se señala:

1. Persona física
    a. Acta de nacimiento
    b. Identificación oficial vigente (INE, pasaporte, cédula profesional).
    c. CURP.
    d. RFC.
    e. Comprobante de domicilio no mayor a tres meses.
    f. Constancia de cumplimiento de obligaciones fiscales.
    g. Constancia de situación fiscal.
    h. Formato de KYC llenado y firmado.
2. Persona moral
    a. Acta constitutiva.
    b. Asambleas protocolizadas cuando se hayan realizado modificaciones relevantes para la operación de la sociedad.
    c. Poderes de representación del representante legal debidamente protocolizados.
    d. Comprobante de domicilio de la persona moral no mayor a tres meses.
    e. RFC de la persona moral.
    f. Constancia de opinión de cumplimiento de obligaciones fiscales.
    g. Constancia de situación fiscal.
    h. Formato de KYC llenado y firmado.
    i. RFC del representante legal.
    j. CURP del representante legal.
    k. Comprobante de domicilio del representante legal.
    l. Identificación oficial vigente del representante legal (INE, pasaporte, cédula profesional).
3. La solicitud se deberá acompañar de un escrito bajo protesta de decir verdad conforme a lo señalado en la fracción IV del artículo 102 del Código de Comercio.
4. Los solicitantes deberán sujetarse y aprobar las evaluaciones de conocimientos en materia de Prestadores de Servicios de Certificación y certificados digitales que PSC Codex considere pertinentes, además de culminar satisfactoriamente los procedimientos que establezca la dirección de recursos humanos.
5. Los equipos de cómputo con los cuales se pretenda operar como Agente Certificador serán auditados por el Profesional Informático de PSC Codex quien deberá verificar que los mismos implementen los controles de seguridad que establece PSC Codex dentro de sus políticas de seguridad.

6. El solicitante deberá contar con espacios físicos adecuados, que implementen medidas de seguridad que garanticen que los certificados digitales serán emitidos en un ambiente confiable.
7. El solicitante deberá contar con un seguro de responsabilidad civil y fianza la cual deberá tener cobertura conforme a los montos señalados en las Reglas Generales a las que deberán sujetarse los PSC.
8. Conocer, aceptar y alinear sus procesos de seguridad a las Políticas de Seguridad establecidas por PSC Codex, así como de su Sistema de Gestión de Seguridad de la Información.

Una vez que el solicitante da cumplimiento a todos los requisitos señalados, se procederá a la firma del contrato correspondiente con PSC Codex.

Actualización de políticas y procesos de seguridad

Las Políticas, procesos y mecanismos de seguridad de PSC Codex consideran revisiones semestrales o anuales según el documento de que se trate y deberá atender a los principios de auditoría interna y proceso de mejora continua que se señalan dentro del Sistema de Gestión de Seguridad de la Información a fin de garantizar una metodología homologada para la revisión de procesos, detección y corrección de no conformidades. Si bien cada uno de los documentos de seguridad tiene considerado su periodo de revisión, el mismo podrá verse modificado y entrar en revisión cuando se presenten modificaciones relevantes en los procesos de seguridad, en la tecnología y/o infraestructura que integra la Autoridad Certificadora y Registradora, ante la presencia de la vulneración de datos o ante modificaciones en el marco normativo que regula la actividad de los PSC.

El Aviso de Privacidad y las Políticas aplicables a la Protección de Datos Personales que permiten dar cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento, también son consideradas dentro de los procesos de revisión y actualización derivados del Sistema de Gestión de Seguridad de la Información.

Los Agentes Certificadores de PSC Codex deberán atender en todo momento las Políticas y procedimientos en materia de Seguridad de la Información que sean publicadas por PSC Codex dentro de sus sitios internos y que sean hechas de su conocimiento. Los Agentes Certificadores deberán entender, aceptar e implementar las políticas de PSC Codex, principalmente las Políticas de Seguridad Física, de Seguridad de la Información, así como los controles señalados en el Sistema de Gestión de Seguridad de la Información.

Una vez que los Agentes Certificadores, cuando se trate de personas morales, se den por enterados de las actualizaciones en políticas y procesos de seguridad implementados por PSC Codex, deberán notificar a PSC Codex el proceso de comunicación que se llevará a cabo con los operadores y señalar las fechas en las cuales entrarán en funcionamiento las nuevas directrices. El tiempo de implementación no podrá ser superior a diez días hábiles.

Confidencialidad de la Información

PSC Codex como parte de su Sistema de Gestión de Seguridad de la Información, implementa una Política de Clasificación de la Información en la cual se establecen los

procedimientos y procesos que se deben de cumplir dentro de la organización para la clasificación y etiquetado de los datos que se recaban como parte del proceso de emisión de un certificado digital.

La implementación de esta Política permite a PSC Codex dar cumplimiento a los requerimientos que se establecen en la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento para el resguardo y gestión de los datos proporcionados por los suscriptores y partes interesadas en el servicio.

Protección de datos personales

PSC Codex como parte de sus procesos organizacionales está comprometido en dar cumplimiento a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares y de su Reglamento, para ello como parte del proceso de emisión de un certificado digital hace del conocimiento de los interesados el Aviso de Privacidad en el cual se establece la finalidad para la cual se están recabando sus datos, en este caso la emisión del certificado digital. Dicho aviso de privacidad ha sido redactado utilizando un lenguaje ciudadano que facilita el entendimiento de los principios que en él se enuncian estructurando su contenido de manera que sea comprensible para el titular de los datos.

El aviso de privacidad deberá ser aceptado por el titular con anterioridad al tratamiento de sus datos, dicha aceptación se dará en primera instancia dentro de la plataforma digital de PSC Codex a través de una casilla de verificación la cual, una vez seleccionada, permitirá continuar con el proceso. Una vez que culmina el proceso de emisión del certificado digital y como parte de la entrega al titular, este deberá de firmar autógrafamente el aviso de privacidad que se le presenta por escrito; con ello, el titular otorga su consentimiento expreso al responsable en medios electrónicos y en medios físicos pudiendo identificar plenamente al titular.

Ahora bien, con la finalidad de poder atender al compromiso que tiene la organización con sus usuarios y del cumplimiento a la Ley Federal de Protección de Datos en Posesión de Particulares y su Reglamento, PSC Codex implementa medidas de seguridad administrativas, técnicas y físicas que permiten proteger los datos personales, además de garantizar que el Aviso de Privacidad dado a conocer es respetado en todo momento. Las medidas de seguridad implementadas por PSC Codex para el tratamiento y resguardo de la información recolectada como parte del servicio de emisión de certificados digitales serán las mismas que se implementan para el manejo de la información organizacional y de sus sistemas. Entre las medidas consideradas por PSC Codex, se encuentra la implementación de las siguientes políticas:

1. Política de Seguridad de la Información.
2. Política de Seguridad Física.
3. Política de Atención a Incidencias de Seguridad de la Información.
4. Política de Control de Acceso a Sistemas de Información.
5. Política de Gestión de Usuarios.
6. Sistema de Gestión de Seguridad de la Información.

En lo que respecta a las medidas de seguridad que se implementan en los entornos digitales se tiene implementada una plataforma basada en roles y perfiles de usuario los cuales tienen bien definidos los permisos de acceso y visualización de la información de

los usuarios. En ese sentido, es importante mencionar que únicamente existen dos perfiles que tienen autorización para visualizar los datos que ingresa el usuario como parte de la solicitud del certificado, uno de ellos es el propio usuario y el otro es el Agente Certificador quien debe de verificar y cotejar que la información que se ha ingresado en el sistema sea pertinente, correcta y conforme fue plasmada en los documentos que presenta el usuario conforme se señala en el proceso de verificación de identidad.

A nivel de base de datos, la protección de datos personales se realiza minimizando el número de usuarios que tienen acceso a la base de datos, siendo el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad los únicos que tienen autorizado el acceso a la visualización de la información almacenada. Ahora bien, aun y cuando el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad son colaboradores con un alto grado de confianza, están sujetos a controles de auditoría donde cualquier tipo de consulta que ejecutan sobre la base de datos genera una pista de auditoría que podrá ser revisada con posterioridad.

En lo que respecta a la transferencia de información entre la Autoridad Registradora, la Autoridad Certificadora y la base de datos es importante mencionar que la transferencia se realiza a través de protocolos seguros donde la información en tránsito se encuentra cifrada utilizando certificados SSL. Adicionalmente, una vez que la información se encuentra dentro de la plataforma de PSC Codex, las comunicaciones se encuentran restringidas a la red interna configurada por PSC Codex.

Es importante mencionar que, en la implementación de las medidas de seguridad administrativas, técnicas y físicas mencionadas se consideran factores relevantes para la operación de los sistemas de PSC Codex, descritas en las Políticas y procedimientos de seguridad, incluyendo el tipo de datos y documentos que se están recabando, procesos de transferencia de datos, condiciones de carga, concurrencia y rendimiento.

Finalmente, en atención a la Ley Federal de Protección de Datos Personales en Posesión de Particulares y su Reglamento todos los colaboradores de PSC Codex ya sean directos o indirectos conocen y están obligados a dar cumplimiento a las medidas de protección de datos personales conforme al procedimiento establecido para el tratamiento de datos personales y su contrato laboral, además de contar con un convenio de confidencialidad el cual se mantendrá vigente por lo menos un año posterior al término de la relación laboral con PSC Codex.

Vulneraciones de datos

PSC Codex considera que se vulnera la seguridad de la información cuando de forma intencionada o no intencionada se pone en riesgo la confidencialidad, integridad o disponibilidad de la información, con lo cual se puede afectar a los titulares de la información. La seguridad de la información puede ser vulnerada en cualquier fase del tratamiento y puede tener origen en cualquiera de los siguientes escenarios:

1. Pérdida o destrucción no autorizada.
2. Robo o copia no autorizada.
3. Uso, acceso o tratamiento no autorizado.
4. Daño, alteración o modificación no autorizada.

Sin importar el motivo por el cual se haya vulnerado la seguridad de la información, PSC Codex detonará los procesos que se establecen dentro de su Política de Atención a

Incidencias de Seguridad de la Información, los cuales permiten desarrollar las acciones necesarias para dar tratamiento a las incidencias presentadas.

Adicionalmente, PSC Codex será responsable de informar a los titulares de la información respecto de la vulneración de la información, así como de las actividades a seguir para determinar la magnitud de la afectación, a fin de que los afectados puedan tomar las medidas correspondientes.

Como parte del proceso de notificación, PSC Codex informará a los titulares al menos lo siguiente:

1. La naturaleza del incidente.
2. Los datos personales comprometidos.
3. Las recomendaciones al titular acerca de las medidas que puede adoptar.
4. Las acciones correctivas realizadas de forma inmediata.
5. Los medios donde puede obtener más información al respecto.

Una vez finalizado el análisis que permita identificar las causas por las cuales se presentó la vulneración de la información, PSC Codex seguirá el proceso de mejora continua establecido como parte de su SGSI, para llevar a cabo las acciones necesarias que permitan incrementar los niveles de seguridad y ayuden a mitigar el riesgo presente en sus sistemas.

Gestión de la seguridad

PSC Codex garantiza a los suscriptores y partes interesadas que la gestión y administración de los procesos asociados a la emisión de Certificados Digitales se realiza de conformidad con las Políticas de Certificación, así como en la presente Declaración de Prácticas en concordancia con los estándares y mejores prácticas de referencia que establece la Secretaría de Economía dentro de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.

En ese sentido, PSC Codex declara que cuenta con infraestructura y desarrollo propios para la integración de su Autoridad Certificadora y por tanto es el único responsable de los aspectos y componentes relacionados con la emisión de certificados digitales. Además, PSC Codex mantienen la responsabilidad y obligación de divulgar el contenido de la presente Declaración de Prácticas entre sus suscriptores, sujetos relacionados y partes interesadas en el servicio.

Para la gestión de la seguridad relaciona con el servicio, la Alta Dirección de PSC Codex a conformado un Comité de Seguridad el cual ha sido el responsable de la definición de la Política de Seguridad de la Información aplicable a los servicios que PSC Codex tiene acreditados como Prestador de Servicios de Certificación, conforme a los criterios definidos en el Sistema de Gestión de Seguridad de la Información PSC Codex hace de conocimiento de sus empleados y colaboradores los diversos documentos relacionados con la Seguridad de la Información y mantiene un constante programa de concientización y capacitación.

Los controles de seguridad aplicables al servicio de emisión de certificados digitales de PSC Codex están documentados en los documentos de seguridad de la información del

servicio, principalmente en el Sistema de Gestión de Seguridad de la Información y el Plan de Seguridad de Sistemas.

Clasificación y gestión de activos

PSC Codex como parte del proceso de implementación de su Sistema de Gestión de Seguridad de la Información, de la Política de Seguridad de la Información, de la Política de Seguridad Física, así como del Análisis de Riesgos se asegura que sus diferentes activos, ya sea información, activos intangibles o equipos que integran la infraestructura de la AC se encuentren clasificados conforme al nivel de criticidad que representan para la operación del servicio de emisión de Certificados Digitales.

En ese sentido, PSC Codex dentro del apartado de activos críticos del "Análisis y Evaluación de Riesgos y Amenazas" ha relacionado aquellos componentes de la AC que por su importancia son considerados como indispensables para la prestación del servicio. Una vez identificados los activos y clasificados conforme a su nivel de criticidad les son aplicadas las políticas de protección de activos relacionadas con cada nivel de riesgo.

Seguridad del personal

PCS Codex como parte de los procesos que se implementan para incrementar la seguridad de la información en lo relativo a su Autoridad Certificadora se asegura que los procesos de contratación, así como la selección de candidatos soportan la integridad de las operaciones de su Autoridad. Para ello, PSC Codex ha desarrollado e implementado el "*Procedimiento de reclutamiento y selección*" el cual establece el procedimiento a seguir durante la contratación de personal.

Ahora bien, particularmente para las vacantes y candidatos a puestos relacionados con la operación de la AC, PSC Codex aplica las siguientes consideraciones:

a. El personal que labora directamente en la gestión y operación de la AC tiene conocimiento experto, experiencia y calificaciones necesarias para las funciones propias del servicio de emisión de certificados digitales. El conocimiento experto en temas relacionados a la AC se puede comprobar mediante constancias y cursos de capacitación, así como por experiencia previa laborando con servicios similares.
b. Los roles de seguridad, así como sus responsabilidades se encuentran definidos en el Sistema de Gestión de Seguridad de la Información y son documentados en el perfil de puesto correspondiente.
c. Los roles de confianza como son el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad son los responsables directos de gestionar las operaciones de la AC y son acreditados ante la Secretaría de Economía.
d. El personal que labora en actividades relacionadas a la AC este sujeto a los controles de Gestión de usuarios definidos en el Plan de Seguridad de Sistemas implicando, entre otros: la separación de actividades, asignación de privilegios mínimos, niveles de acceso, comprobación de antecedentes y referencias, así como la capacitación y concientización respecto de las actividades inherentes a su puesto.

e. El personal asignado a los roles de confianza se encuentra libre de cualquier conflicto de interés que pueda obstaculizar la operación de la AC de PSC Codex.

Seguridad física y ambiental

PSC Codex implementa una Política de Seguridad Física la cual tiene como objeto el establecer los lineamientos, procedimientos y mecanismos de seguridad que se deberán de atender dentro de la organización y las instalaciones donde realice cualquier tipo de actividad con la finalidad de asegurar que sus activos de información, de infraestructura, de comunicaciones y de recursos humanos, entre otros, se mantienen íntegros y disponibles para garantizar la disponibilidad de los servicios que soportan.

Los lineamientos que se establecen en materia de seguridad física, a su vez, deben ayudar a generar las condiciones propicias que permitan dar cumplimiento a los procesos establecido dentro del Sistema de Gestión de Seguridad de la Información, así como a la consecución de los objetivos de seguridad de la información. Desde la perspectiva de PSC Codex la seguridad física de su infraestructura como Prestador de Servicios de Certificación está directamente relacionada con la seguridad de la información al ser el primer elemento de control a través del cual se establecen limitaciones de acceso a los equipos dentro de los cuales se realizan los procesos de emisión de certificados digitales, sellos digitales de tiempo y de constancias de conservación de mensajes de datos.

En ese sentido, el grupo de trabajo de seguridad de PSC Codex, con la finalidad de asegurar que la presente Política ayuda en la consecución de los objetivos organizacionales, así como en la protección de activos, tiene la responsabilidad de ejecutar las siguientes tareas:

1. Mantener la Política de Física de PSC Codex actualizada conforme a los riesgos y retos que representan las condiciones operativas, así como factores externos a la organización.
2. Generar lineamientos para la administración de los procedimientos de seguridad aplicables a las instalaciones dentro de las cuales se desarrollen actividades relacionadas a los servicios acreditados por PSC Codex.
3. Garantizar que la infraestructura de PSC Codex se mantiene segura.
4. Gestionar y actualizar los procedimientos de acceso a las áreas seguras o de procesamiento de las instalaciones donde se realicen operaciones de PSC Codex como PSC.
5. Definir perímetros de control de acceso a las áreas seguras tanto de los centros de datos como de las oficinas administrativas para resguardar la información de los servicios que PSC Codex considera como información crítica.
6. Asegurar la protección de la infraestructura crítica, definida en el Análisis y Evaluación de Riesgos y Amenazas implementando correctamente los protocolos de seguridad que establecen los centros de datos contratados.

El detalle de los controles de acceso y procedimientos de seguridad física y ambiental que se tienen implementados en los centros de datos y oficinas administrativas de PSC

Codex se pueden consultar a detalle en el documento de la "*Política de Seguridad de la Información*".

Gestión de las operaciones

PSC Codex dentro de sus obligaciones como Prestador de Servicios de Certificación esta obligado a asegurar que los componentes de su Autoridad Certificadora, tanto en software como en hardware, operan correctamente y con un limitado nivel de fallo. Por lo anterior y atendiendo a lo establecido en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, PSC Codex implementa, entre otras, las siguientes medidas:

1. La infraestructura física de la AC se resguarda en dos centros de datos.
2. Se establecen procedimientos de acceso a las oficinas administrativas y centros de datos.
3. Se utilizan sistemas antivirus en los componentes de la AC.
4. Se utilizan herramientas de detección de vulnerabilidades.
5. Las instalaciones de los centros de datos cuentan con sistemas de detección y protección de intrusiones.

Adicionalmente, la infraestructura tecnológica que forma parte de la AC de PSC Codex cuenta con mantenimientos preventivos programados lo que permite extender el tiempo de vida útil de sus componentes. El mantenimiento lo lleva a cabo personal de PSC Codex que cuenta con los conocimientos técnicos necesarios para realizar este tipo de tareas.

El Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad monitorean constantemente la demanda del servicio de emisión de certificados digitales para conocer si la capacidad instalada de infraestructura es suficiente para continuar soportando el servicio o se requiere escalar los componentes de infraestructura a fin de continuar brindando el servicio que suscriptores y sujetos relacionados esperan.

Gestión de acceso a los sistemas

PSC Codex garantiza que el acceso a su infraestructura física y a los componentes lógicos que integran su Autoridad Certificadora se encuentra limitado al personal de confianza designado por la organización y que se encuentra acreditado como parte de los elementos humanos ante la Secretaría de Economía.

Como ya se ha señalado, la infraestructura física de PSC Codex se encuentra ubicada dentro de los centros de datos que se tienen contratados a los cuales únicamente tiene acceso el personal acreditado por PSC Codex y que para el ingreso a las instalaciones debe de cumplir con todos los lineamientos que señalan los propios centros de datos para el acceso a sus instalaciones. Además, los centros de datos, como parte de la Política de Seguridad Física tienen implementados sistemas de detección y protección de intrusiones los cuales permiten contar con los elementos necesarios para recibir las alertas relacionadas con intentos de acceso no autorizados a las instalaciones y particularmente a las áreas seguras de los centros de datos.

En la protección de los elementos lógicos implementa elementos como firewall para restringir las comunicaciones que ingresan a la Autoridad Certificadora, donde adicionalmente se hace uso de routers y switches para implementar mayores niveles de seguridad para la emisión de certificados digitales. El Firewall, además, tiene restringidos todos aquellos protocolos que no están relacionados con los servicios que presta PSC Codex como Prestador de Servicios de Certificación para limitar las vulnerabilidades que puedan presentarse en ese sentido.

Respecto de la seguridad implementada en las comunicaciones, mediante el uso de los routers, switch y firewalls PSC Codex garantiza que la infraestructura de su Autoridad Certificadora tiene restringidas las comunicaciones a equipos que integran dicha Autoridad y que toda comunicación con los suscriptores y partes interesadas se da mediante las interfaces de servicios que PSC Codex ha desarrollado, a través de las cuales se completa el proceso de emisión de un certificado digital.

La operación del servicio implica que el personal de confianza que opera el servicio de emisión de certificados digitales se encuentra plenamente identificado en todo momento dentro de los sistemas con medidas que permiten separar las funciones dentro del sistema. La operación de la AC también implica que las actividades se encuentran monitoreadas constantemente con la finalidad de detectar, registrar y reaccionar a cualquier intento de acceso no autorizado que pueda poner en riesgo la operación del servicio.

Implementación y mantenimiento de sistemas confiables

El sistema, componentes y servicios de software que componen la Autoridad Certificadora de PSC Codex han sido desarrollados e implementados por personal de la organización que sigue las mejores prácticas en el desarrollo de aplicaciones y sistemas con la finalidad de asegurar que los sistemas cuentan con las medidas de seguridad necesarias para proteger la seguridad de la información generada como parte del servicio.

Durante el proceso de levantamiento de requerimientos del sistema, ya sea durante el desarrollo inicial o durante la implementación de mejoras, particularmente en la etapa de diseño del sistema el equipo de PSC Codex analiza e identifica los componentes o procesos que pudieran generar vulnerabilidades en la operación del servicio y construye la solución corrigiendo dichas vulnerabilidades.

Adicionalmente, para una mejor gestión del ciclo de vida del software del sistema de emisión de certificados digitales, PSC Codex hace uso de herramientas de control de versionamiento con la cual se puede tener un seguimiento puntual de los cambios que se realizaron en cada una de las liberaciones realizadas como parte del proceso de mejora continua del sistema.

Plan de continuidad de negocio

PSC Codex entiende que cualquier proceso que se ejecute en medios electrónicos requiere de la definición de un Plan de Continuidad de Negocio y Recuperación ante Desastres el cual tiene como finalidad establecer los procedimientos que la organización deberá seguir en caso de la presencia de incidencias o desastres que pongan en riesgo la continuidad de los servicios que PSC Codex tienen acreditados como Prestador de Servicios de Certificación.

En ese sentido, PSC Codex ha elaborado el documento del Plan de Continuidad de Negocio y Recuperación ante Desastres el cual entre otras cosas considera:

- Afectación al funcionamiento de los sistemas y/o software.
- Incidente de seguridad que afecte la operación de los sistemas y/o software.
- Afectación a las ubicaciones de los centros de datos donde se ubica la infraestructura tecnológica de PSC Codex.
- Robo de los Datos de Creación de Firma Electrónica de los Certificados Digitales del Prestador de Servicios de Certificación.
- Demás casos que por su naturaleza pongan en riesgo el servicio acreditado.
- El mantenimiento y ejecución de pruebas periódicas para garantizar la funcionalidad del Plan de Continuidad.

Dicho Plan de Continuidad está planteado de forma general para los servicios que PSC Codex tiene acreditados como Prestador de Servicios de Certificación y contiene consideraciones específicas para los servicios de emisión de certificados digitales, sellos digitales de tiempo y constancias de conservación de mensajes de datos.

El detalle completo podrá ser consultado en el documento del Plan de Continuidad de Negocio y Recuperación ante Desastres.

Cese de actividades de la AC

El cese de actividades, temporal o definitivo, de la Autoridad Certificadora de PSC Codex podrá llevarse a cabo a petición de PSC Codex, por considerarlo conveniente a sus intereses, o como parte de una resolución dictada por la Secretaría de Economía conforme a los supuestos que se establecen en Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Cese temporal de actividades

El cese temporal de actividades a petición de PSC Codex únicamente podrá llevarse a cabo cuando la infraestructura tecnológica que compone su Autoridad Certificadora requiera ser actualizada y se requiera detener los servicios de emisión de certificados digitales. Para poder llevar a cabo la suspensión, PSC Codex notificará con al menos 30 días de anticipación a la Secretaría de Economía y el tiempo de suspensión no podrá exceder de 15 días hábiles desde la fecha de inicio de la suspensión hasta la fecha de reanudación de actividades.

Concluido el periodo determinado de la suspensión PSC Codex deberá entregar a la Secretaría de Economía los documentos que se establecen en las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación que, a consecuencia de la actualización de infraestructura, hayan sido modificado o actualizado.

Adicionalmente, la suspensión temporal de actividades de PSC Codex como Autoridad Certificadora, podrá llevarse a cabo por resolución de la Secretaría de Economía cuando se configure alguno de los supuestos que se establecen en los artículos 24, 25 y 26 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.

Ahora bien, independientemente de la causa que derive en la suspensión temporal de actividades, PSC Codex deberá realizar las siguientes actividades:

1. Suspender la emisión de certificados digitales.
2. Notificar a los usuarios del servicio el tiempo de la suspensión.
3. Suspender el registro de solicitudes de emisión de certificados.
4. Emitir un mensaje dentro de las secciones relacionadas a la emisión de certificados en su página web donde se indique el periodo y motivo de la suspensión.
5. Mantener en todo momento activos los servicios de validación del estatus del certificado, ya sea a través del protocolo OCSP o las listas CRL.

PSC Codex se asegurará de minimizar las afectaciones a sus suscriptores y partes interesadas como parte del cese temporal del servicio, además de asegurarse de mantener mecanismos que permitan a los interesados asegurar la autenticidad de los certificados digitales emitidos.

Terminación de la Autoridad Certificadora

PSC Codex podrá dar cesar o dar por terminadas sus funciones como Autoridad Certificadora autorizado por la Secretaría de Economía cuando por circunstancias económicas, políticas, sociales o por su propio interés decida que no puede continuar prestando de manera confiable el servicio de emisión de certificados digitales, así como los procesos relacionados con la validación y verificación del estatus de los certificados emitidos.

Como parte del proceso de terminación de la Autoridad Certificadora, PSC Codex atenderá los lineamientos que se establecen en la Regla 18 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, el artículo 16o. Del Reglamento y de la fracción VI del artículo 104 del Código de Comercio. PSC Codex, conforme lo establece la normativa correspondiente y previo el pago de derechos correspondiente, notificará a la Secretaría de Economía con al menos cuarenta y cinco días hábiles de anticipación su intención de cesar actividades como Autoridad Certificadora.

Durante el periodo de referencia para la terminación de la AC, PSC Codex pondrá a disposición de la Secretaría de Economía los archivos de registro y de auditoría que

permitan verificar que la AC de PSC Codex estuvo operando dentro de la normativa aplicable, para que la misma determine si la propia Secretaría o quien de los PSC acreditados para la emisión de certificados digitales resguardará dicha información; PSC Codex pondrá especial atención en la transferencia y disponibilidad de los mecanismos conocidos para la verificación del estatus de los certificados que emitió como Prestador de Servicios de Certificación. Si no fuera posible mantener activo el servicio del protocolo OCSP, PSC Codex se asegurará de continuar emitiendo las listas CRL hasta su último día de operaciones, momento en el cual transferirá dichas listas a la Secretaría o al PSC que se haga cargo de sus registros.

Además de la notificación a la Secretaría de Economía, PSC Codex buscando minimizar las afectaciones a las partes interesadas en su servicio de emisión de certificados digitales, ejecutará las actividades siguientes:

1. Notificar y poner a disposición de sus suscriptores y partes interesadas la información concerniente a la terminación del servicio, así como los procedimientos que permitan reducir las afectaciones que puedan generarse como parte del servicio.
2. Pondrá a disposición de las partes interesadas a través de su página de internet la información relativa a la terminación de su Autoridad Certificadora.
3. Notificará a la Autoridad Registradora que tuviera habilitada respecto de la terminación de la Autoridad Certificadora y el correspondiente cese de actividades.
4. Suspenderá los accesos de los Agentes Certificadores a la plataforma de la Autoridad Registradora.
5. Solicitará a la Autoridad Registradora el envío de los expedientes que se integraron como parte del servicio de emisión de certificados digitales.
6. La información relacionada con el servicio de emisión de certificados digitales, así como la relacionada con la operación de PSC Codex será resguardada y almacenada conforme a la normativa aplicable.
7. Una vez que la Secretaría de Economía defina quien será el responsable de la información de PSC Codex, se notificará a los usuarios, además de transmitir la información relevante de este proceso.
8. PSC Codex se asegurará de mantener operativos los servicios de emisión de CRL y de OCSP hasta su último día de operaciones.
9. PSC Codex mantendrá vigentes los seguros de responsabilidad civil y las fianzas solicitadas para su operación como PSC, hasta por lo menos un año posterior a la fecha de terminación de su Autoridad Certificadora.

Finalmente, PSC Codex se asegurará que las llaves privadas de los datos de creación de firma de la AC sean eliminadas de los módulos criptográficos y cualquier medio electrónico de tal manera en que no puedan ser recuperadas. La Secretaría de Economía determinará la procedencia de la revocación de los certificados digitales emitidos para la Autoridad Certificadora de PSC Codex; en caso de que la SE determine la revocación PSC Codex notificará a suscriptores, sujetos relacionados y partes interesadas la decisión, así como la revocación de aquellos certificados que al momento de la determinación de la SE aún se mantuvieran vigentes.

Registro de información relativa a la operación del servicio

Registros físicos

Como parte de la operación de la Autoridad Certificadora para la emisión de certificados digitales, PSC Codex integra registros de información que resguardan los datos a partir de los cuales se generó el certificado digital. En ese sentido, se integra un expediente físico en el cual se incluyen las copias cotejadas de los documentos que presentó el solicitante para la emisión del certificado, mismo que queda bajo la responsabilidad del Agente Certificador que emitió dicho certificado y quien deberá de resguardar en un espacio seguro los expedientes y tenerlos identificables en caso de que sean requeridos por la autoridad.

El Agente Certificador tendrá la obligación de verificar que la documentación que fue cargada en el sistema, a la hora de generar la solicitud del certificado, sea legible y permita identificar los datos presentes en el documento correspondiente. En caso de que los documentos que fueron cargados en el sistema no sean legibles, los Agentes Certificadores no podrán emitir el certificado y deberán solicitar al usuario que proporcione documentos legibles.

Los expedientes físicos integrados por los Agentes Certificadores deberán ser resguardados por un periodo de al menos diez años a partir de la emisión del certificado digital y en caso de dejar de operar como Agente Certificador los expedientes deberán ser remitidos a las oficinas administrativas de PSC Codex para la continuidad del resguardo.

En el caso de la autoridad registradora de PSC Codex, los expedientes físicos serán resguardados en las áreas seguras designadas en las oficinas administrativas y están bajo la responsabilidad del Agente Certificador y el Profesional Jurídico que se tengan acreditados ante la Secretaría de Economía.

Registros informáticos

Además de los registros físicos, PSC Codex conforme a su modelo operativo ha diseñado e implementado una base de datos de información, en la cual se registran aquellos datos relativos a los solicitantes de la emisión de un certificado digital. El resguardo de los datos de información se centra en el resguardo de los datos del usuario conforme son plasmados en la solicitud del requerimiento y que son integrados dentro del certificado digital.

Adicionalmente, se generan y almacenan los metadatos necesarios para vincular los datos de generación del certificado con los documentos soporte que se cargan en la plataforma como parte del proceso de solicitud de un certificado; además, PSC Codex almacena los datos del certificado como son el número de serie y la fecha y hora de emisión para cualquier cotejo que deba de realizarse con posterioridad.

Los sistemas de información de PSC Codex, en especial la base de datos donde se resguardan los datos de los solicitantes de un certificado, se rige conforme a los controles de acceso a sistemas de información definidos por PSC Codex y son

responsabilidad del Profesional Informático quien es el encargado de establecer los procedimientos para asegurar la Seguridad de la Información del servicio.

Proceso de auditoría

El programa de auditorías internas de PSC Codex establece que esta actividad se llevará a cabo de manera anual o en el momento que se considere necesario cuando los cambios en materia tecnológica así lo requieran o cuando se detecten vulnerabilidades graves en los componentes de la arquitectura tecnológica de los servicios de emisión de certificados digitales, sellos digitales de tiempo o constancias de conservación de mensajes de datos.

El programa de auditoría deberá ser de conocimiento de las áreas que gestionan, administran y operan los servicios que PSC Codex tiene autorizados como Prestador de Servicios de Certificación, a fin de que coordinen actividades y puedan facilitar oportunamente la información que requieran los auditores asignados. Durante el proceso de auditoría, además de los criterios y alcance definidos en el programa de auditoría, se deberán de considerar los resultados de las auditorías anteriores a fin de verificar que las observaciones y no conformidades encontradas hayan sido solventadas.

Ahora bien, en lo que respecta a las auditorías que se realizan sobre los sistemas de información relacionados con el servicio de emisión de certificados digitales, es importante conocer que cada uno de los componentes cuenta con un registro activo de actividades que en conjunto con las herramientas de monitoreo permite al Profesional Informático y al Auxiliar de Apoyo Informático de Seguridad conocer el comportamiento del sistema, además de identificar posibles amenazas o errores dentro de los procesos.

Los registros de auditoría se componen de los siguientes elementos:

1. Registro de eventos de la Autoridad Certificadora.
2. Registro de eventos de la Autoridad Registradora.
3. Eventos de bitácora relacionados con el servicio.
4. Sistema de directorios de la Autoridad Certificadora.
5. Registro de eventos de la base de datos.
6. Registro de eventos del software EMSISOFT.

Estos elementos son analizados al menos una vez a la semana por el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad para verificar que no se estén presentando errores o incidencias que puedan poner en riesgo la operación en el servicio. De encontrar registro de algún evento relacionado con la seguridad de la información deberán seguir los procedimientos descritos en la “Política de atención de incidentes de seguridad de la información”.

Es importante mencionar que con independencia de las revisiones que periódicamente se realizan a los registros de auditoría, los componentes de seguridad que se implementan como parte de la infraestructura de la autoridad certificadora permiten identificar, a través del monitoreo constante, riesgos asociados a la seguridad de la

información donde se emiten alertas a los encargados del servicio respecto de los riesgos potenciales.

Cumplimiento de la legislación aplicable

El marco jurídico mexicano establece los lineamientos de operación de los servicios que los Prestadores de Servicios de Certificación pueden emitir, donde parte fundamental de los requerimientos se centra en la seguridad de la información.

Entre la normativa aplicable a PSC Codex como Prestador de Servicios de Certificación y particularmente para el servicio de emisión de certificados digitales, se encuentran los ordenamientos siguientes:

1. Ley de Firma Electrónica Avanzada.
2. Disposiciones Generales de la Ley de Firma Electrónica Avanzada.
3. Código de Comercio.
4. Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación.
5. Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación.
6. Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.
7. Ley Federal de Protección de Datos Personales en Posesión de Particulares.
8. Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

CRL de PSC Codex

El objetivo de la publicación de la CLR de PSC Codex es generar un ambiente de interoperabilidad con los suscriptores y partes interesadas en implementar servicios de firma electrónica avanzada permitiendo conocer de forma periódica si el estatus de un certificado ha sido modificado durante su vigencia. Como se señala en el Rfc 5280 una Autoridad Certificadora puede generar una o más CRL's cada una de las cuales podrá tener un alcance específico que dependerá del propósito de emisión de cada una de las listas.

PSC Codex como parte de la operación de su Autoridad Certificadora, inicialmente emitirá una única CRL, la cual será consultable aquí y cuyo objetivo será listar todos aquellos certificados emitidos que se encuentran vigentes y que han sido revocados conforme a los motivos señalados en el apartado de "Motivos de revocación" del presente documento.

Atendiendo a los requerimientos de las Reglas Generales a las que deberán de sujetarse los Prestadores de Servicios de Certificación, así como a los procedimientos señalados en el Rfc 5280, la CRL de PSC Codex será publicada en periodos no mayores a 24 horas.

PSC Codex se reserva el derecho a emitir CRL's adicionales si las necesidades de su operación así lo requieren y publicará en su página de internet el alcance específico de

cada una de las listas publicadas, así como la dirección electrónica en la que estarán disponibles para su consulta.

Estructura de la CLR

La estructura de la CRL publicada por PSC Codex es emitida conforme a las consideraciones y recomendaciones que establece el Rfc 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Dentro de la información que forma parte de la CRL emitida y firmada por la AC de PSC Codex, destacan los datos siguientes:

1. Número de serie del certificado revocado.
2. Fecha y hora de revocación.
3. Nombre del emisor de la CRL, en este caso PSC Codex.
4. Fecha y hora de emisión de la CRL.
5. Algoritmo de firma utilizado.
6. Fecha en que se emitirá la siguiente CRL.
7. La CRL estará firmada por PSC Codex, como emisor, con sus datos de Creación de Firma Electrónica.

La CRL de PSC Codex estará disponible para consulta de los suscriptores y partes interesadas en la dirección electrónica

PSC Codex

PSC Codex declara que es una organización legalmente establecida conforme a los señalamientos de la Ley General de Sociedades Mercantiles y cuya constitución fue protocolizada ante Fedatario Público y se encuentra inscrita en el Registro Público de Comercio con el Folio Mercantil Electrónico N-2021001797. PSC Codex declara que puede operar como Prestador de Servicios de Certificación una vez que ha dado cumplimiento a los requerimientos que establece la normativa aplicable y ha sido acreditado por la Secretaría de Economía para actuar como tal para la emisión del servicio de Emisión de Certificados Digitales.

PSC Codex declara contar con un seguro de responsabilidad civil, así como de las fianzas que señalan las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación para hacer frente a cualquier compromiso derivado de la gestión y operación del servicio de emisión de certificados digitales. Sin menoscabo de lo anterior, PSC Codex declara contar con la suficiente capacidad y estabilidad financiera para operar adecuadamente el servicio que le ha sido acreditado por la Secretaría de Economía.