Documento

Política de certificación

PSC Codex

Versión 1.2

2 de septiembre del 2024

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 estas 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 Política 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 Política de Certificación 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.
- Disposiciones Generales de la 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.
- Norma Oficial Mexicana NOM-151-SCFI-2016, Requisitos que deben observarse para la conservación de mensajes de datos y digitalización de documentos.
- Ley Federal de Protección de Datos Personales en Posesión de Particulares.

- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los 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 Política de Certificados Digitales 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 las Políticas de Certificación de los servicios relativos a la emisión de certificados digitales, y que contienen o elaboran la Política de Certificados, 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 Política de Certificación 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.

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).

La presente Política de Certificación se emite en concordancia con los procesos, procedimientos y políticas que se incluyen como parte de la Declaración de Prácticas de Certificación de la Autoridad Certificadora, consultable en la dirección electrónica https://www.psccodex.com/practicas_certificados/, así como del Modelo Operacional de la Autoridad Certificadora y Registradora de PSC Codex.

Identificación

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 está 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: 2.16.484.101.10.316.100.10.1.1.1.1.1.0

Inicio de operaciones

Con fecha de 26 de octubre del 2022 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.

Publicada la acreditación, PSC Codex inicio operaciones del servicio de emisión de Certificados Digitales con fecha 27 de mayo de 2024.

Publicación de la Política de Certificación

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

Usuarios y aplicabilidad

La presente Política de Certificación Tiempo 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.

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 de las Políticas de Certificación que se incluye en los Certificados Digitales emitidos por PSC Codex es: 2.16.484.101.10.316.100.10.1.1.1.1.1.0

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

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.

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.

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.

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.

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 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 certificados y autoridades registradoras, 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.
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 con 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 a la que aplique su Firma electrónica avanzada 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.

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 o Autoridades Registradoras 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 CRL 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, se debe de llevar a cabo el procedimiento que se conoce como Ceremonia de generación de los Datos de Creación de Firma de la Autoridad Certificadora de PSC Codex, la cual 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.

Durante la Ceremonia el certificado de la AC de PSC Codex 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. Adicionalmente, 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.

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.

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*".

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 se asegura contar con los elementos mencionados, para iniciar el proceso de respaldo es necesario cargar los archivos de respaldo en el directorio *"file system"* del dispositivo y utilizar las llaves de Seguridad del Security World para descifrar 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 pone a disposición de sus suscriptores y partes interesadas la llave pública del certificado de su Autoridad Certificadora la cual se encuentra disponible en el portal de internet de PSC Codex, en la dirección https://www.psccodex.com/certificados/autoridad-certificadora/, así como en el portal de la Secretaría de Economía, en la dirección https://psc.economia.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 y algoritmo a utilizar

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 https://psc.economia.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.

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.
2. Revocación de claves.
3. Función hash obsoleta.
4. Longitud de claves no segura.

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.

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.

Elegibilidad para la emisión de un certificado digital

PSC Codex como Autoridad Certificadora acreditada por la Secretaría de Economía para la emisión de certificados digitales ha determinado que los sujetos susceptibles de recibir un certificado son todas aquellas personas físicas que actúen por su propio derecho o en representación de una persona moral.

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 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.

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 de firma electrónica avanzada 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 Codex y es extensible a su Autoridad Registradora, 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 con 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 el Agente Certificador 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 para personas físicas, 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.

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 máxima de dos años contados a partir de la fecha de generación del certificado, de conformidad con el artículo 109 fracción del Código de Comercio. PSC Codex podrá emitir certificados digitales con una vigencia menor a dos años a petición de los suscriptores.

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.

Renovación presencial

El proceso de renovación presencial requiere que el suscriptor o sujeto relacionado complete el proceso descrito en el apartado denominado “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.

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 esta relacionado con la identidad biométrica 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 la 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.

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.

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 usuario realizará el proceso de revocación. Para poder ejecutar el proceso de revocación, el solicitante deberá acreditar su personalidad mediante una identificación oficial, tratándose de suscriptores personas físicas o de sujetos relacionados.

A continuación, se relacionan los motivos de revocación 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.

Motivo	Documentación adicional	¿Quién puede realizar el proceso?
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
Cese de actividades de una empresa / Baja de la Empresa / Cierre permanente de una empresa.	Acuse del aviso de suspensión de actividades ante IMSS/SAT	Patrón acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización) y documento que acredite la relación laboral
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 o cambio de denominación o razón social	Resolución judicial por el procedimiento de rectificación de acta de nacimiento, pre acta, nueva acta de nacimiento y anterior. Escritura pública protocolizada ante fedatario en la cual se establece el cambio de denominación.	Usuario acreditándose con identificación oficial vigente (INE, Pasaporte, Carta de naturalización)
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).

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.

Interoperabilidad de los certificados de PSC Codex

PSC Codex garantiza a sus suscriptores, partes interesadas y otros Prestadores de Servicios de Certificación acreditados por la Secretaría de Economía, que los certificados que emite a través de su Autoridad Certificadora serán compatibles con los sistemas que por su propio derecho e interés desarrollen y que como parte de su arquitectura consideren el estándar X.509 como base de funcionamiento.

Adicionalmente, PSC Codex hace del conocimiento de suscriptores, partes interesadas, Prestadores de Servicios de Certificación y autoridades, que los servicios de validación del estatus del certificado, como son el OCSP y la CRL, serán

considerados como servicios de acceso público con la finalidad de garantizar que las transacciones que se realicen con los certificados emitidos por la AC de PSC Codex cuenten con plena validez y certeza.

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: https://www.app.psccodex.com/crl

Administración y operación de la AC

Autoridades Registradoras o Agentes Certificadores

Las Reglas 21 y 25 de las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación permiten a PSC Codex 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 o Autoridad Registradora deberán entregar la documentación y cumplir con los requisitos que se señalan.

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.

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 la Política 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, así como de su Sistema de Gestión de Seguridad de la Información.

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 aparatado 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.

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 Física*".

Gestión de las operaciones

PSC Codex dentro de sus obligaciones como Prestador de Servicios de Certificación está 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 de Sellado Digital de Tiempo 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.

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 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 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 continúa 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.

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.

Cese definitivo de actividades

El cese definitivo de actividades podrá darse a petición de PSC Codex, cuando así sea conveniente para la organización, o cuando la Secretaría de Economía así lo resuelva conforme a los criterios que se establecen en el artículo 27 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación. En caso de que el cese de actividades sea de manera voluntaria, PSC Codex, previo pago de los derechos correspondientes, notificará a la Secretaría de Economía con al menos cuarenta y cinco días de anticipación su decisión.

Una vez que se ha notificado a la Secretaría de Economía, PSC Codex se asegurará de 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. Además de la notificación que realizará PSC Codex, la información relativa al cese de actividades de la Autoridad Certificadora estará disponible para la consulta de las partes interesadas a través de la página de internet de PSC Codex.

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 al PSC que se haga cargo de sus registros.

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.

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 los Particulares

Calendario de revisiones

PSC Codex dentro de sus procesos organizacionales ha establecido que la revisión a la Política de Certificación de su Autoridad Certificadora se realizará de forma anual. Ahora bien, las revisiones podrán realizarse de forma extraordinario si las condiciones tecnológicas, sociales, ambientales o de cualquier otra naturaleza así lo requieran.

Fecha de la revisión	Versión revisada	Responsable (Nombre y firma)	Observaciones
03/06/2022			
03/06/2023			
03/06/2024			
03/06/2025			
03/06/2026			

Control de versiones del documento

Fecha de la revisión	Versión revisada	Responsable (Nombre y firma)	Observaciones
03/01/2022	1.0	(firmado anteriormente) _____ **Profesional Informático/ Auxiliar de Apoyo Informático de Seguridad** Juan Francisco Estrada Garfias (firmado anteriormente) _____ **Profesional Jurídico** Susana Nicole Chávez Facio	Documento inicial que será presentado a la Secretaría de Economía con la finalidad de obtener la acreditación como Prestador de Servicios de Certificación. .
01/08/2022	1.1	(firmado anteriormente) _____ **Profesional Informático/ Auxiliar de Apoyo Informático de Seguridad** Juan Francisco Estrada Garfias (firmado anteriormente) _____ **Profesional Jurídico** Susana Nicole Chávez Facio	Se realizan las correcciones correspondientes al documento de conformidad con las observaciones generadas por la Secretaría de Economía como parte del proceso de acreditación. Se sustituyó la imagen del Firewall
02/09/2024	1.2	_____ **Profesional Informático/ Auxiliar de Apoyo Informático de Seguridad** Juan Francisco Estrada Garfias _____ **Profesional Jurídico** Cintya Lopez Rodriguez	Se realizan las correcciones correspondientes al documento de conformidad con las observaciones generadas por la Secretaría de Economía como parte del proceso de acreditación. Se sustituyó la imagen del Firewall