Política de Certificados Aplicable a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

OID: 2.16.484.101.10.316.2.5.1.1.1.1.1.2

Versión 1.4

Tabla de Contenidos

1. Administración de la Documentación

I. Manejo de Versiones

El presente documento será considerado válido y con vigencia siempre que los cambios hayan sido autorizados y aprobados por los responsables definidos en la siguiente sección

El presente documento deberá ser revisado dos veces al año, lo cual no implica una actualización del mismo.

II. Control de Versiones

El manejo de versiones para la documentación sigue el cumplimiento de políticas definidas para la asignación de un número de versión, de acuerdo a:

Se incrementa un número entero cuando

- Un cambio o mejora grande ocurre en la documentación.
- Un conjunto de características, que han sido planeadas, han sido implementadas.
- La estructura del documento cambia.
- Si el contenido del documento cambia en un 40% será necesario incrementar el número de versión con un número entero.

Se incrementa con un decimal sobre la versión del documento cuando

Se incrementa para distinguir múltiples liberaciones de la actualización de la documentación.
Este número indica mejoras o cambios menores en el contenido de la documentación.
Si el contenido del documento cambia en un porcentaje menor al 40%, será necesario incrementar el número de versión con un número decimal.

VERSIÓN	FECHA DE	CAMBIO EN EL DOCUMENTO
1.0	25 OCTUBRE 2010	DOCUMENTO INICIAL
1.1	4 ABRIL 2011	ACTUALIZACIONES EN FUNCION DE RECOMENDACIONES REALIZADAS EN PREVENTORIO Y DICTAMEN POR PARTE DE LA SECRETARIA DE ECONOMIA
1.2	MAYO 2018	PROCEDIMIENTO DE RENOVACION DE CERTIFICADOS

1.3	**30 DIC 2021**	**ACTUALIZACIÓN DE CALENDARIO**
1.4	**12 JULIO 2024**	**ACTUALIZACIÓN DE CALENDARIO , REVISIÓN Y ACTUALIZACIÓN DE PROTECCIÓN DE DATOS Y ALMACENAMIENTO DE EXPEDIENTES DE SUSCRIPTORES**

III. Lista de Distribución

Las copias en papel, medio magnético y electrónico de este documento están almacenadas en las siguientes localidades.

LOCALIDAD	DIRECCIÓN	RESPONSABLE	MEDIO DE ALMACENAMIENTO
CDMX	INSURGENTES SUR 2375	OLGA GARCIA	MAGNETICO Y PAPEL
CDMX	KIO INTERLOMAS	MOISES BAUTISTA	MAGNETICO Y PAPEL

IV. Calendario de Revisiones del Documento

El documento se revisará al menos una vez al año para verificar que el contenido sea aplicable y funcional a la Infraestructura de Clave Pública, lo que no implica una actualización del mismo.

FECHAS PROGRAMADAS DE FUTURAS REVISIONES
30-12-2020
30-12-2021
30-12-2022
30-12-2023
30-12-2024
30-12-2025

2. Introducción

La Política de Certificados es un conjunto de reglas que establece la aplicabilidad de los Certificados a un determinado grupo de personas (físicas o morales) con requisitos de seguridad comunes. Además establece los procesos y procedimientos que se emplean en la emisión, la

entrega, el uso y la administración de los Certificados y las obligaciones y responsabilidades de los participantes de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

2.1. Definiciones y Acrónimos

Término	**Definición**
Autoridad Certificadora	La Autoridad Certificadora es la entidad que se encarga de la emisión, la administración y la revocación de los certificados digitales conforme a lo descrito en la Declaración de Prácticas de Certificación.
Agente Certificador	Es la persona física o moral que actúa a nombre y por cuenta de la Autoridad Certificadora y tiene la función de comprobar 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.
Certificado	Todo Mensaje de Datos u otro registro que confirme el vínculo entre un Firmante y los datos de creación de Firma Electrónica.
Llave pública	Las llaves criptográficas, datos o códigos únicos que utiliza el destinatario para verificar la autenticidad de la firma electrónica del firmante.
Datos de creación de Firma electrónica (llave privada)	Son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
Firma electrónica	Los datos en forma electrónica consignados en un Mensaje de Datos, o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al Firmante en relación con el Mensaje de Datos e indicar que el Firmante aprueba la información contenida en el Mensaje de Datos, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio.
Firma Electrónica avanzada	Aquella Firma Electrónica que cumpla con los requisitos contemplados en las fracciones I a IV del artículo 97. En aquellas disposiciones que se refieran a Firma Digital, se considerará a ésta como una especie de la Firma Electrónica.

Destinatario	La persona designada por el Emisor para recibir el Mensaje de Datos, pero que no esté actuando a título de Intermediario con respecto a dicho Mensaje. De acuerdo al artículo 89 del Código de Comercio
Mensaje de datos	La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología. De acuerdo al artículo 89 del Código de Comercio
Firmante	La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona a la que representa De acuerdo al artículo 89 del Código de Comercio
Titular del certificado	Se entenderá a la persona a cuyo favor fue expedido el Certificado De acuerdo al artículo 89 del Código de Comercio
Dispositivo de verificación de firma electrónica	El programa o sistema informático que sirve para aplicar los datos de verificación de firma electrónica.
PSC	Prestador de Servicios de Certificación (La persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso)
CP	Política de Certificación por sus siglas en inglés.
Token	Dispositivo electrónico de seguridad utilizado para el resguardo y almacenamiento de las llaves criptográficas del usuario.
Suscriptor	Se entiende por suscriptor, a toda aquella persona física nacionalidad mexicana o extranjero con residencia temporal o permanente en México, o moral, o administrador de un dominio de sitio web, titular de un certificado digital, que voluntariamente confía y hace uso de su certificado digital emitido por la Autoridad Certificadora. En el momento que un titular de un certificado digital decida voluntariamente confiar y hacer uso de su certificado digital, le será aplicable la Declaración de Prácticas de Certificación.
Parte que confía	La persona que, siendo o no el Destinatario, actúa sobre la base de un Certificado o de una Firma Electrónica.

2.2. Información General

La acreditación como Prestador de Servicios de Certificación (PSC) es otorgada por la Secretaría de Economía. La función de los PSC es emitir Certificados, con los términos y los requisitos que establece el Código de Comercio, con el fin de que los Certificados otorguen certeza jurídica y seguridad informática en la celebración de actos de comercio por medios electrónicos (Internet) entre los participantes de estos actos.

SeguriData Privada S.A. de C.V. ha decidido implementar una Autoridad Certificadora para constituirse como Prestador de Servicios de Certificación, la cual dotará a sus suscriptores de Certificados que, para efectos de sus actividades, necesiten plasmar su voluntad mediante el uso de la Firma electrónica avanzada.

La presente Política de Certificados contiene las políticas que regirán el funcionamiento y operación de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V., contiene el conjunto de reglas que indican la aplicabilidad, las responsabilidades y el uso que le pueden dar los titulares de un certificado, así como la gestión que se emplea sobre los Certificados emitidos.

La estructura de esta Política de Certificados está basada en lo dispuesto por la IETF (Internet Engineering Task Force) en el documento de referencia RFC 3647, denominado como “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. Asimismo, para el desarrollo de su contenido, se han tenido en cuenta los requisitos establecidos en la especificación Técnica ETSI (European Telecommunications Standards Institute) TS 102 042 V2.1.1 (2009-05) – “Electronic Signatures and Infrastructure (ESI); Policy requirements for certification authorities issuing public key certificates”.

La presente Política de Certificados tiene por objeto el permitir que electrónicamente se autentique la identidad del firmante, se asegure la integridad de los documentos firmados electrónicamente y se evite el no repudio de los mismos.

Esta Política de Certificados asume que el lector conoce los conceptos que se manejan en una Infraestructura de Clave Pública, conceptos de Certificados, así como los conceptos relacionados con la Firma electrónica avanzada.

La representación esquemática de los componentes involucrados en la Infraestructura de Clave pública es la que se muestra en la figura 1.

En el nivel superior de la figura, se ubica la Autoridad Certificadora raíz y núcleo de confianza perteneciente a la Secretaría de Economía.

El segundo nivel corresponde a la Autoridad Certificadora constituida como Prestador de Servicios de Certificación por parte de SeguriData Privada S.A. de C.V., en la cual, se emiten los Certificados de identidad y Firma electrónica avanzada a los suscriptores.

El tercer nivel corresponde a los Agentes Certificadores, encargados de la identificación y autenticación de los solicitantes, y gestión de la emisión de los Certificados, así como también de la revocación de los mismos.

Finalmente, el cuarto nivel corresponde a los solicitantes, que al momento de adquirir su certificado, son considerados como suscriptores de la Infraestructura de Clave Pública que tiene como núcleo de confianza a la Autoridad Certificadora de la Secretaría de Economía.

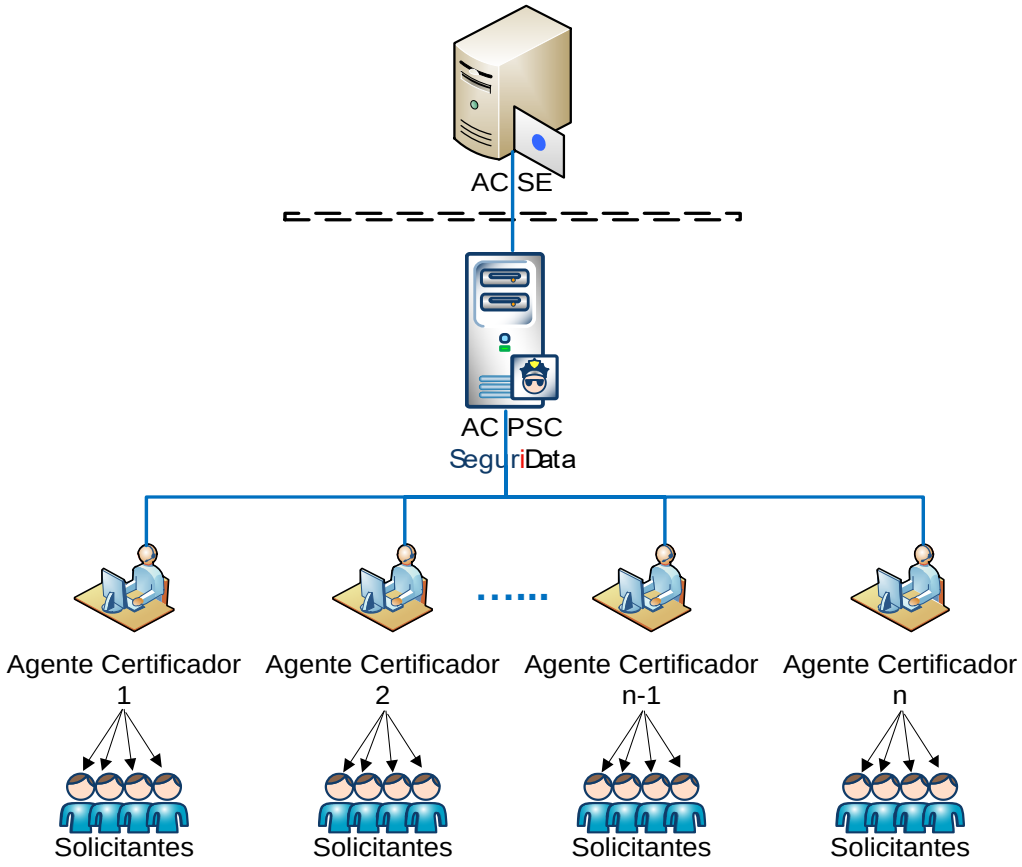


Figura 1

2.3. Nombre del Documento e Identificación

A continuación se proporciona el nombre y los datos de identificación del presente documento.

Nombre del documento	Política de Certificados aplicables a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.
Versión del documento	1.3
Autor	SeguriData Privada S.A. de C.V.
Estado del documento	En operación
Fecha de emisión	4/04/2011
Fecha de inicio de uso	6/10/2012
Fecha de expiración	No es aplicable
Identificador Digital de Objetos – OID (Object Identifier Digital)	2.16.484.101.10.316.2.5.1.1.1.1.1.2
Localización (URL) de la Política de Certificados	https://psc.seguridata.com/docs/doc06.pdf
Declaración de Prácticas de Certificación Asociada	Declaración de Prácticas de Certificación Aplicables a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

2.3.1. Determinación de Cambios en esta Política de Certificados

Las modificaciones propuestas o las nuevas aportaciones a incluir en esta Política de Certificados deberán, previa a su aprobación, ser contrastadas con la Declaración de Prácticas de Certificación, a fin de asegurar que sean soportados estos cambios.

No se podrán realizar cambios que no sean soportados por la Declaración de Prácticas de Certificación. Deberá, en todo caso, contemplarse una actualización de la Declaración de Prácticas de Certificación.

2.4. Personas y Entidades Participantes en la Infraestructura de Clave Pública

Las entidades que conforman los roles de los participantes dentro de la Infraestructura de Clave Pública son:

- Autoridad Certificadora
- Agentes Certificadores llamados así en SeguriData a las Autoridades Registradoras
- Entidades Finales
    - Solicitantes
    - Suscriptores
- Partes que Confían

2.4.1. Autoridad Certificadora

La Autoridad Certificadora Raíz perteneciente a la Secretaría de Economía es el núcleo de confianza de la Infraestructura de Clave Pública en asuntos del orden comercial.

Los datos de la Autoridad Certificadora Raíz son:

Nombre Distintivo	CN = Autoridad Certificadora Raíz de la Secretaria de Economía OU = Dirección General de Normatividad Mercantil O = Secretaria de Economía C = MX S = Distrito Federal L = Alvaro Obregon PostalCode = 01030
Número de serie	01
Periodo de validez	Desde sábado, 07 de mayo de 2005 07:00:00 p.m. hasta miércoles, 07 de mayo de 2025 07:00:00 p.m.
Estado	Operativa

Huella digital (SHA-1)	34 d4 99 42 6f 9f c2 bb 27 b0 75 ba b6 82 aa e5 ef fc ba 74

En el segundo nivel se encuentra la Autoridad Certificadora de SeguriData Privada S.A. de C.V. constituida como Prestador de Servicios de Certificación, la cual es la entidad encargada de la emisión y administración de los Certificados que está conformada bajo los términos de la presente Política de Certificados.

Los datos de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. perteneciente a la Infraestructura de Clave Pública es la siguiente:

Nombre Distintivo	CN = Autoridad Certificadora de SeguriData Privada S.A. de C.V. OU = Prestación de Servicios de Certificación O = SeguriData Privada S.A. de C.V. C = MX, S = Distrito Federal L = Alvaro Obregon PostalCode = 01000
Número de serie	El número de serie será determinado una vez que se acredite a SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación.
Periodo de validez	El periodo de validez será determinado una vez que se acredite a SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación.
Estado	Operativa
Huella digital (SHA-1)	La huella digital (sha-1) será determinada una vez que se acredite a SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación.

2.4.2. Agentes Certificadores

Los Agentes Certificadores están constituidos por las oficinas que disponga la Autoridad Certificadora de SeguriData Privada S.A. de C.V. para realizar la expedición de los Certificados.

En caso de requerirse, el Agente Certificador podrá trasladarse a diferentes ubicaciones geográficas de la República Mexicana para certificar a solicitantes y conforme avance el tiempo, se estarán abriendo más oficinas en otras partes de la República Mexicana, y en el mismo Distrito

Federal, llamándolos agentes certificadores externos, notificando a la Secretaría de Economía los nuevos Agentes Certificadores y sus oficinas, así como publicando en el Sitio WEB los Agentes Certificadores

La misión de los Agentes Certificadores es asistir a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. en los procedimientos y trámites relacionados con los solicitantes para su identificación, registro y autenticación, garantizando con esto que el solicitante es quien dice ser y que posee la clave privada correspondiente. Además, una vez emitido el Certificado a los solicitantes, tienen la posibilidad de solicitar la revocación de los mismos.

2.4.3. Entidades Finales

Las Entidades Finales o usuarios están constituidos por solicitantes de Certificados y por suscriptores de Certificados.

Los solicitantes de Certificados, son usuarios potenciales que buscan tener un certificado de la Infraestructura de Clave Pública, los cuales presentan su solicitud y la información correspondiente que los identifique ante un Agente Certificador para su validación.

Los suscriptores o titulares de Certificados son los usuarios que ya cuentan con su certificado emitido por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. como Prestador de Servicios de Certificación.

2.4.4. Parte que Confía

Las personas que, siendo o no el Destinatario, actúan sobre la base de un Certificado o de una Firma Electrónica avanzada.

2.5 Tipos de Certificados que se emiten

Los tipos de Certificados que se emiten están en función del nivel de seguridad de los mismos. Se tienen Certificados con nivel de Seguridad Media y Alta.

Los Certificados tienen diferentes niveles de seguridad, dependiendo el ámbito para el cual son utilizados y el que el suscriptor decida solicitar. La política de Certificados es aplicable para los dos tipos de Certificados.

Los niveles de seguridad son: Certificado con nivel de seguridad media y Certificado con nivel seguridad alta. El nivel de seguridad alta de un certificado, es cuando se generan los Datos de Creación de Firma electrónica avanzada en un dispositivo de seguridad criptográfico (Token compatible con FIPS 140-2 Nivel 3).

Los Certificados con nivel de seguridad media, son cuando se entrega el Certificado en el repositorio del sistema operativo, mediante los CGI's del Sitio Web de la Autoridad Certificadora, o cuando el solicitante acude a las oficinas del Agente Certificador a generar su requerimiento, y guarda sus Datos de Creación de Firma electrónica avanzada en una unidad de almacenamiento extraíble (memoria USB).

Para todos los certificados emitidos se sigue un proceso de validación de la identidad del Solicitante por parte del Agente Certificador, en el cual, los datos que el solicitante ingresa en su requerimiento, los coteja contra la documentación presentada, previo cotejo contra los originales de dicha documentación.

Los certificados serán utilizados para actos de comercio, y los procesos de validación, restricciones y límites en su uso, están delimitados por la estructura del certificado, donde se detallan sus usos y por la Política de Certificados aplicable.

La vigencia de los certificados emitidos para suscriptores no podrá ser superior a 2 años, contados a partir de la fecha en que sean expedidos, de acuerdo al Código de Comercio, y por el tamaño de la llave de los mismos, de acuerdo a las recomendaciones del NIST National Institute of Standards and Technology, basado en la evolución de seguridad en el tamaño de las llaves.

Los certificados se emiten para personas físicas con nacionalidad mexicana, o extranjeros con residencia temporal o permanente en México, para personas extranjeras con residencia en el extranjero que trabajen para una empresa Mexicana y para los representantes de personas morales.

Los tipos de Certificados se emiten en función del nivel de seguridad de los mismos. Se tienen Certificados con nivel de Seguridad Media y Alta.

Los Certificados SSL Secure Site protegen la transferencia de datos confidenciales en sitios web, intranets y extranets. Incluye cifrado de hasta 256 bits. Es un certificado digital de tipo SSL que garantiza la identidad del sitio, la integridad y privacidad de la información transmitida a través de Internet entre un sitio Web y un navegador, quedando libre de ser robada o modificada durante su envío.

CARACTERÍSTICAS DEL CERTIFICADO DE SEGURIDATA PARA EMISIÓN DE CERTIFICADOS SSL

Para la emisión de certificados SSL de sitio, el certificado emitido a SeguriData, necesita tener al menos las siguientes características:

Núm. de Serie: Recomendable Generación aleatoria de un tamaño de hasta 20 bytes
Alg. de firma: sha256 con RSA
Datos del Sujeto: Country - PrintableString
Organization - PrintableString ó UTF8String
Common Name - PrintableString ó UTF8String
Llave: RSA de al menos 2048 Bits
Recomendable RSA de 3072 bits y hasta 4096
Extensiones:
Key Usage (2.5.29.15)
Crítica: Sí
Valor: 0x06 = Firma de Certificados, Firma de CRL
Basic Constraints (2.5.29.19)
Crítica: Sí
Valor: CA = True
Path Length Constraint: 0
Subject Key Identifier (2.5.29.14)
Crítica: No
Valor: Hash (sha1) de la llave pública de SeguriData
Certificate Policies (2.5.29.32)
Crítica: No
Valor: Identificador de la política (OID)
CPS (1.3.6.1.5.5.7.2.1)
URL indicando la localización del CPS
Authority Info Access (1.3.6.1.5.5.7.1.1)
Crítica: No
Valor: OCSP (1.3.6.1.5.5.7.48.1)
URL indicando dirección y puerto del OCSP
Authority Key Identifier (2.5.29.35)
Crítica: No
Valor: Hash (sha1) de la llave pública de la AC Raíz de la Secretaría de Economía

CARACTERÍSTICAS DE LOS CERTIFICADOS DE SITIO SSL "ESTÁNDAR"

Los certificados de SSL para sitio existen en dos "versiones": la versión estándar y la versión de validación extendida. Los certificados "estándar" se subdividen a su vez en certificados de validación de dominio (DV) y los certificados de Validación de Organización (OV). La diferencia está administrativamente en la orientación de las validaciones: la comprobación de que la empresa tiene la posesión del dominio o la comprobación de la constitución de la organización.

Aunque el CA Browser Forum ha recomendado una forma explícita de diferenciar entre un certificado OV y un DV, no muchos emisores de certificados SSL han seguido dichas recomendaciones. La diferencia entre ambos certificados es la política de emisión: orientada a la validación del dominio o la orientada a la validación de la organización.

Los certificados "estándar" de SSL para sitio generados por SeguriData tendrían las siguientes características mínimas:

Núm. de Serie: hasta 20 bytes aleatorios
Alg. de firma: sha256-RSA
Datos del Sujeto: Country - PrintableString
State - PrintableString ó UTF8String

Locality - PrintableString ó UTF8String
Organization - PrintableString ó UTF8String
CommonName - PrintableString ó UTF8String – Este campo debe tener la url principal del certificado de sitio

Llave: RSA de al menos 2048 Bits
Recomendable RSA de 3072 bits

Extensiones:

Subject Alternative Name (2.5.29.17)
Crítica: No
Valor: Uno o varios DNS, por ejemplo:
*.ge-mechanics.com
www.ge-mechanics.com
(debe contener el dns principal idéntico al CommonName)

Basic Constraints (2.5.29.19)
Crítica: No
Valor: CA = False (Es decir, "End Entity")
Path Length Constraint: None

Key Usage (2.5.29.15)
Crítica: Sí
Valor: 0xA0 = Digital Signature, Key Encipherment

CRL Distribution Point (2.5.29.31)
Crítica: No
Valor: Distribution Point Name (URL)

Certificate Policies (2.5.29.32)
Crítica: No
Valor: Policy Identifier: (OID de la política de Certificación)
CPS (1.3.6.1.5.5.7.2.1)
URL donde se encuentra el CPS
User Notice (1.3.6.1.5.5.7.2.2) - OPCIONAL
URL donde se encuentra el aviso legal

Enhanced Key Usage (2.5.29.37)
Crítica: No
Valor: Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)

Authority Key Identifier (2.5.29.35)
Crítica: No
Valor: Hash (sha1) de la llave pública de la AC de SeguriData

Authority Info Access (1.3.6.1.5.5.7.1.1)
Crítica: No
Valor: OCSP (1.3.6.1.5.5.7.48.1)
URL y puerto donde se encuentra el respondedor de OCSP
Certification Authority Issuer (1.3.6.1.5.5.7.48.2) - OPCIONAL
URL donde se encuentra el certificado de la AC

Subject Key Identifier (2.5.29.14) - OPCIONAL
Crítica: No
Valor: Hash (sha1) de la llave pública del certificado de sitio

CARACTERÍSTICAS DE LOS CERTIFICADOS SSL DE VALIDACIÓN EXTENDIDA

Núm. de Serie: Hasta 20 bytes aleatorios
Alg. de firma: sha256-RSA
Datos del Sujeto: Business Category - PrintableString ó UTF8String - OPCIONAL
Country - PrintableString
State - PrintableString ó UTF8String
Locality - PrintableString ó UTF8String
Street - PrintableString ó UTF8String
Organization - PrintableString ó UTF8String
Common Name - PrintableString ó UTF8String – Este campo debe tener la url principal del certificado de sitio
Llave: RSA de al menos 2048 Bits
Recomendable RSA de 3072 bits
Extensiones:
Subject Alternative Name (2.5.29.17)
Crítica: No
Valor: Uno o varios DNS, por ejemplo:
*.ge-mechanics.com
www.ge-mechanics.com
(debe contener el dns principal idéntico al CommonName)
Basic Constraints (2.5.29.19)
Crítica: No
Valor: CA = False
Path Length Constraint: None
Key Usage (2.5.29.15)
Crítica: Sí
Valor: 0xA0 = Digital Signature, Key Encipherment
CRL Distribution Points (2.5.29.31)
Crítica: No
Valor: Distribution Point Name (URL)
Certificate Policies (2.5.29.32)
Crítica: No
Valor: Policy Identifier: (OID de la política de Certificación)
CPS (1.3.6.1.5.5.7.2.1)
URL donde se localiza el CPS
User Notice (1.3.6.1.5.5.7.2.2) - OPCIONAL
URL donde se encuentra el aviso legal
Enhanced Key Usage (2.5.29.37)
Crítica: No
Valor: Server Authentication (1.3.6.1.5.5.7.3.1)
Client Authentication (1.3.6.1.5.5.7.3.2)
Authority Key Identifier (2.5.29.35)
Crítica: No
Valor: Valor: Hash (sha1) de la llave pública de la AC de SeguriData
Authority Info Access (1.3.6.1.5.5.7.1.1)
Crítica: No
Valor: OCSP (1.3.6.1.5.5.7.48.1)
URL=http://ocsp.globalsign.com/rootr2
Certification Authority Issuer (1.3.6.1.5.5.7.48.2) - OPCIONAL
URL donde se encuentra el certificado de la AC
Subject Key Identifier (2.5.29.14) - Opcional
Crítica: No

```
        Valor: Hash (sha1) de la llave pública del certificado de sitio
SignedCertificateTimestampList (1.3.6.1.4.1.11129.2.4.2) - Opcional
    Crítica: No
      Valor: Estampillas del pre-registro del certificado, según
             el RFC 6962 (Certificate Transparency)
```

2.6 Uso de los Certificados Digitales

Los certificados entregados son compatibles con los usos listados a continuación:

1. Firma electrónica avanzada
2. Firma de Correo Electrónico Seguro
3. Firma de código (aplicaciones)
4. Autenticación de usuarios
5. Certificados SSL protección de sitios web

2.6.1 Uso Apropiado de los Certificados Digitales

Los certificados digitales emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación, son expedidos para ámbitos comerciales y tienen como finalidad lo siguiente:

Autenticación de usuarios: garantizar la identidad del titular del certificado digital al momento de realizar cualquier transacción electrónica con un tercero de confianza, el certificado digital dará la certeza de que la comunicación electrónica se realiza con la persona que dice ser. El titular de un certificado digital podrá acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado digital y de la llave privada asociada al mismo.

Firma electrónica Avanzada: permite al titular firmar trámites o documentos de manera electrónica. El certificado digital permitirá la sustitución de la firma autógrafa por la firma electrónica. Todo titular de un certificado digital emitido por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. obtendrá el valor de plena prueba legal para los documentos electrónicos donde éste aplique su firma electrónica, respecto al hecho de que asegura la integridad, no repudio y autenticidad de los mismos.

Correo Electrónico Seguro: Permite al titular firmar y cifrar correos electrónicos, garantizando así la autenticidad, no repudio, integridad y confidencialidad de los mensajes de correo electrónico.

Firma de Código Fuente: Los certificados de firma de Código Fuente generan una Firma electrónica avanzada que ofrece autenticidad de la fuente del código y garantiza la integridad del código, los sistemas operativos, aplicaciones de software, dispositivos y redes inalámbricas necesitan una Firma electrónica avanzada que asegure que el código no dañará ni interrumpirá los servicios.

Certificado SSL: Se emite para brindar seguridad al visitante de una página web, una manera de decirles a sus clientes que el sitio es auténtico, real y confiable para ingresar datos personales. Las siglas SSL responden a los términos en inglés (Secure Socket Layer), el cual es un protocolo de seguridad que hace que sus datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada. El que los datos viajen cifrados, nos referimos a que se emplean algoritmos matemáticos y un sistema de claves que sólo son identificados entre la persona que navega y el servidor. Al tener un certificado SSL confiable, nuestros datos están encriptados, en ese momento podemos asegurar que nadie puede leer su contenido. Todo esto nos lleva a entender que la tecnología que brinda un certificado SSL es la transmisión segura de información a través de internet, y así confirmar que los datos están libres de personas no deseadas. Para poder utilizar un certificado SSL, en su página web, es de vital importancia que el servidor de Internet que usted contrató, soporte SSL.

2.6.2 Limitantes y Restricciones en el Uso de los Certificados

Los Certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., están sujetos únicamente a lo que la presente Política de Certificados y la Declaración de Prácticas de Certificación establecen.

Los Certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., solamente podrán utilizarse para autenticar (acreditación de identidad) al titular, para Firma electrónica avanzada (integridad y no repudio de lo firmado), para correo electrónico, para firma de código fuente y para garantizar sitios seguros SSL.

Los Certificados no podrán ser empleados para actuar como Agente Certificador y/o Autoridad Certificadora, es decir, para firmar otros Certificados, ni para firmar listas de Certificados revocados.

3. Administración de la Política de Certificados

Responsable de la Administración de la Política de Certificados	
Nombre	SeguriData Privada S.A. de C.V.
Correo electrónico	ac@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.
Teléfono	(55) 3098-0700
Fax	(55) 3098-0702

Persona de Contacto	
Nombre	Oficial de Seguridad
Correo electrónico	oficial.seguridata@seguridata.com
Dirección	Insurgentes Sur 2375 Piso 3 Colonia Tizapán, Delegación Álvaro Obregón. C.P. 01000, México, Distrito Federal.

4. Obligaciones y Responsabilidades de los Participantes de la Infraestructura de Clave Pública

En este subcomponente se describen las obligaciones y responsabilidades que aplican a cada uno de los participantes involucrados en la Infraestructura de Clave Pública.

4.1. Obligaciones

4.1.1. Obligaciones de la Autoridad Certificadora

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. actuará relacionando a un determinado suscriptor con su clave pública mediante la expedición de un Certificado.

El detalle de todas las obligaciones a las que estará sujeta la Autoridad Certificadora de SeguriData Privada S.A. de C.V. se encuentra plasmada en su correspondiente Declaración de Prácticas de Certificación.

La Autoridad Certificadora puede confiar en Agentes Certificadores para los procesos de identificación y autenticación del solicitante del Certificado. En los casos en que la Autoridad Certificadora haya confiado en un Agente Certificador para realizar la identificación y la autenticación del suscriptor. La Autoridad Certificadora correrá con toda la responsabilidad de la identificación y la autenticación de sus suscriptores.

No obstante lo anterior, se exige que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. lleve a cabo revisiones regulares, de obligado cumplimiento, de los Agentes Certificadores para asegurar que cumplen con sus obligaciones según el acuerdo aplicable, (incluyendo las tareas de identificación y autenticación) y esta Política de Certificados. SeguriData Privada S.A. de C.V. debe asegurar que todos los aspectos de los servicios que ofrecen y gestionan dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. son acordes en todo momento con esta Política de Certificados.

Sin perjuicio de todo lo anterior, se considera relevante mencionar que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. está obligada a prestar los servicios relacionados con la Firma electrónica avanzada, dentro de los cuales se encuentran:

- Proporcionar la infraestructura operacional, servicios de certificación, servicios de revocación y servicios de validación que incluyen el Directorio X.500 y el servicio OCSP.
- Usar productos confiables y sistemas protegidos contra manipulaciones o modificaciones no autorizadas, que pueden asegurar su seguridad técnica y criptográfica.
- Conservar toda la información y documentos relacionados con los Certificados emitidos durante un lapso de al menos 5 (CINCO) años desde su emisión.

- Llevar a cabo los esfuerzos razonables para emplear al personal con la calificación, conocimientos y experiencia necesarios para llevar a cabo los servicios de certificación y aplicar las medidas de seguridad fijadas en la Política de Certificados.
- Publicar su certificado de Autoridad Certificadora en https://psc.seguridata.com/
- Realizar sus operaciones en conformidad a la Declaración de Prácticas de Certificación.
- Sus Datos de Creación de Firma Electrónica avanzada son usados sólo en conexión con la firma de sus Certificados y Listas de Revocación de Certificados.
- Aprobar o rechazar las solicitudes de certificados de acuerdo a lo que marca la Declaración de Prácticas de Certificación vigente.
- Emitir Certificados conforme a la información proporcionada por el solicitante en el momento de su emisión y que esté libre de errores en la captura de datos.
- Revocar Certificados de acuerdo a lo que marca la Declaración de Prácticas de Certificación, asimismo de publicar y actualizar la Lista de Certificados Revocados con la frecuencia estipulada.
- Contar con un servicio de validación en línea que implemente el protocolo OCSP para la verificación del estado de un Certificado determinado.
- Contar con CRL para revisar estado de revocación de los Certificados expedidos.

4.1.2. Obligaciones de los Solicitantes de Certificados

Es obligación de los solicitantes de Certificados cumplir con la presente Política de Certificados, incluyendo:

- Proporcionar toda la información que marca el procedimiento de solicitud de Certificado.
- Proporcionar información veraz para realizar la comprobación de su identidad.
- Aceptar las condiciones y términos que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. dispone en la presente Política de Certificados para los Certificados.

4.1.3. Obligaciones de los Agentes Certificadores

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. puede designar Agentes Certificadores específicos para realizar la identificación, la autenticación, la solicitud de emisión de Certificado y las funciones de revocación definidas por esta Política de Certificados. Cualquier Agente Certificador debe realizar sus funciones y obligaciones conforme a la Política de Certificados.

Las obligaciones de los Agentes Certificadores incluyen:

- Atender las solicitudes de emisión de Certificados.
- Mantener y administrar toda la documentación de apoyo relacionada con el uso de los Certificados en un lugar seguro dentro de una gaveta cerrada con llave.
- Atender las peticiones de revocación de Certificados.
- Cumplir con su Acuerdo de Agente Certificador, la Política de Certificados y la Declaración de Prácticas de Certificación vigentes.
- Someterse a las auditorías periódicas que se establezcan y en su caso cumplir con los requerimientos y recomendaciones que de ellas deriven.
- Seguir la política de privacidad descrita en la Declaración de Prácticas de Certificación.
- Seguir las reglas específicas sobre la identificación, la autenticación y la revocación contenida en esta Política de Certificados.

Sin embargo, los agentes certificadores afrontarán cualquier responsabilidad derivada de la falsificación, la falsedad o cualquier otra clase de engaño intencional cometido durante la identificación y el proceso de autenticación en el que consiste la actividad del mismo.

4.1.4. Obligaciones de los Suscriptores

Es obligación de los suscriptores cumplir con la presente Política de Certificados, el Acuerdo de Suscriptor y la Declaración de Prácticas de Certificación, incluyendo:

- Cumplir total y verazmente con toda la información y procedimientos requeridos en relación con la identificación y requisitos de autenticación relevantes para el Certificado emitido según esta Política de Certificados.

- Revisar el Certificado emitido y asegurarse de que toda la información dispuesta allí es completa y exacta y notificar inmediatamente a la Autoridad Certificadora o al Agente Certificador en el caso de que el Certificado contenga cualquier inexactitud.
- Conservar y utilizar de forma correcta su par de claves de acuerdo a la normatividad vigente.
- Proteger y custodiar su clave de anulación, su clave privada y su Certificado asociado, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Proteger el dispositivo Token criptográfico, según sea el caso, empleando las medidas necesarias para evitar su pérdida, revelación, alteración o uso no autorizado.
- Respetar las condiciones y términos firmados durante la solicitud de Certificado.
- 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.
- Abandonar el uso de su par de claves en el caso de que la Autoridad Certificadora notifique al suscriptor que la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. ha sido comprometida.

4.2. Responsabilidades

4.2.1. Responsabilidades de la Autoridad Certificadora

SeguriData Privada S.A. de C.V. como encargada de la Autoridad Certificadora responderá en el caso de incumplimiento de las obligaciones contenidas en la presente Política de Certificados, y conforme a lo establecido en la Declaración de Prácticas de Certificación:

- La Autoridad Certificadora de SeguriData Privada S.A. de C.V. garantiza el cumplimiento de las obligaciones descritas en este documento.
- Asegurar que no exista información falsa en el Certificado y que sea del conocimiento por los Agentes Certificadores que aprueban las solicitudes de Certificados.

- Actuar con diligencia profesional en las tareas inherentes a la administración de la solicitud de Certificado y emisión del Certificado.
- Garantizar que su firma electrónica cumple con todos los requerimientos materiales descritos en la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y uso de los repositorios se lleven a cabo de acuerdo a lo estipulado en la Declaración de Prácticas de Certificación.

4.2.2. Responsabilidad de los Suscriptores

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que sus suscriptores aseguren que:

- Ninguna persona distinta al suscriptor ha tenido acceso a su clave privada.
- Todas las declaraciones efectuadas ante el Agente Certificador durante la solicitud de su Certificado son verdaderas.
- Toda la información a la que aplique su Firma electrónica avanzada es verdadera.
- Cada Firma electrónica avanzada ha sido generada usando su clave privada correspondiente a la clave pública incluida en su Certificado; que dicho certificado ha sido aceptado y está operacional, es decir, está vigente y no ha sido revocado al momento de la generación de la Firma electrónica avanzada.
- La Firma electrónica avanzada se utiliza exclusivamente para propósitos autorizados y legales conforme a lo estipulado en la Declaración de Prácticas de Certificación de la Autoridad Certificadora de SeguriData Privada S.A. de C.V...

4.2.3. Responsabilidad del Agente Certificador

Los Agentes Certificadores asumirán toda responsabilidad sobre la correcta identificación de los solicitantes de Certificados, así como la validación de la información proporcionada, y el resguardo de la documentación en un lugar seguro en una gaveta bajo llave.

4.3. Limitación de Responsabilidad

Las limitaciones de responsabilidad suponen la exclusión de responsabilidad por daños y perjuicios fortuitos o imprevistos directos o indirectos.

4.3.1. Exclusión de Responsabilidad

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no asume ninguna responsabilidad cuando se encuentre ante cualquiera de estas circunstancias:

- Si el Certificado y/o llave privada bajo el control del reclamante ha sido comprometido por mala conservación, falta de confidencialidad, falta de protección contra el acceso, la revelación, el descubrimiento o el uso no autorizado del par de llaves o de cualquier contraseña o datos de activación adicionales para controlar el acceso.

- Si el Certificado bajo el control del reclamante fuera emitido como consecuencia de cualquier falsedad o falsificación de los hechos proporcionados por el suscriptor para generar el Certificado.

- Si el Certificado bajo el control del reclamante hubiera expirado o hubiera sido revocado, y este hecho hubiera sido publicado en https://psc.seguridata.com/ antes de la fecha de las circunstancias que den lugar a cualquier reclamación.

- Si el Certificado bajo el control del reclamante ha sido modificado o cambiado de cualquier modo o usado incumpliendo los términos de esta Política de Certificados, de la Declaración de Prácticas de Certificación o del Acuerdo del Suscriptor.

- Si el Certificado bajo el control del reclamante fue emitido infringiendo la normatividad aplicable.

- Si se ha desarrollado hardware, software, o algoritmos matemáticos, que conviertan en insegura la criptografía de clave pública, siempre que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. haga uso de prácticas comercialmente razonables para protegerse contra incumplimientos en la seguridad que sean resultado de tal hardware, software, o algoritmos.

- El fallo de uno o más sistemas informáticos, de infraestructura de las comunicaciones, de procesamiento o resguardo de la información, o de cualquier sub-componente de los sistemas precedentes, que no esté bajo el control exclusivo de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. y/o sus subcontratistas o proveedores de servicio, siempre que SeguriData Privada S.A. de C.V. use métodos comercialmente razonables de protección contra tales perturbaciones.

- Uno o más de los acontecimientos siguientes: Un desastre natural (incluyendo sin restricción, inundación, terremoto, u otra causa natural o meteorológica relacionada);

huelga; guerra, insurrección u hostilidades militares abiertas; legislación adversa o acción gubernamental, prohibición, embargo, o boicot; revueltas o perturbaciones civiles; incendio o explosión; epidemia catastrófica; embargo o restricción comercial; cualquier falta de disponibilidad de las telecomunicaciones o integridad; incluyendo obligaciones legales, sentencias de un tribunal competente al que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. sea, o pueda ser sujeta; y cualquier acontecimiento o circunstancia fuera del control de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

- Por el uso indebido de la información contenida en el Certificado.

4.4. Responsabilidades Económicas

4.4.1. Indemnización por Parte de la Autoridad Certificadora

Estipulado en la sección 14.9 de la Declaración de Prácticas de Certificación.

4.4.2. Indemnización por Parte de los Suscriptores

Al grado permitido por la Declaración de Prácticas de Certificación aplicables a la Autoridad Certificadora de SeguriData Privada S.A. de C.V., los suscriptores indemnizarán a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. por:

- Falsedad o mala representación de información proporcionada en la solicitud de Certificado.
- Omisión de revelar un hecho destacado en la solicitud de Certificado, si la omisión fue realizada negligentemente o con la intención de engañar a una persona o al Agente Certificador.
- Errores en la protección de su clave privada, en el uso de un sistema de confianza, o en la toma de las precauciones necesarias para prevenir el compromiso, pérdida, entrega, modificación o uso no autorizado de su clave privada.
- El uso de parte del suscriptor de un nombre (incluyendo sin limitación un nombre común, nombre de dominio, o correo electrónico) que infrinja los derechos de propiedad intelectual de un tercero.

5. Publicación y Responsabilidades de Repositorio

5.1. Actualización de la Política de Certificados

La última versión autorizada de este documento de Política de Certificados de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. está en todo momento disponible al público en general en la página https://psc.seguridata.com.

5.2. Repositorios

SeguriData Privada S.A. de C.V. es responsable de administrar el repositorio de Certificados

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no mantiene copias de los Datos de Creación de Firma electrónica avanzada asociados con los Certificados emitidos por ella.

5.3. Frecuencia de Publicación de CRL

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. debe generar una CRL cada 24 horas, y tiene el compromiso de mantenerla actualizada, incluyendo todos los Certificados revocados desde la última actualización.

5.4. Comprobación de OCSP

El servicio de OCSP es en línea, por lo que se consulta directamente del repositorio de claves públicas.

Cualquier parte involucrada en una transacción electrónica que haga uso de Certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., debe verificar el estado de los certificados contra el OCSP de la misma Autoridad Certificadora.

5.4.1. Disponibilidad de la OCSP

La Autoridad Certificadora ofrece el servicio de consulta en línea del estatus de revocación de un certificado, disponible en:

- https://psc.seguridata.com/

5.5. Control de Acceso

La información publicada sobre la Declaración de Prácticas de Certificación, Política de Certificados, y OCSP es de dominio público. Este acceso es de sólo lectura. A través del Sitio WEB.

6. Identificación y Autenticación

En este componente se describen los procedimientos que utilizan los Agentes Certificadores para autenticar la identidad y/u otros atributos de un usuario solicitante de un Certificado antes de la emisión del Certificado.

Este componente también aborda las prácticas de nombres, incluyendo el reconocimiento de los derechos de marca registrada en algunos nombres.

Además, el componente establece los procedimientos para autenticar la identidad y los criterios de aceptación de los solicitantes de entidades que desean convertirse en Agentes Certificadores u otras entidades que actúan o interactúan en la Infraestructura de Clave Pública.

También describe cómo se autentican las partes que soliciten emisión de claves o revocación.

6.1. Denominación

Este subcomponente incluye los siguientes elementos con respecto a la asignación de nombres y la identificación de los suscriptores:

- Tipos de nombres asignados al sujeto, tales como nombres distintivos basados en X.500;
- Si los nombres tienen que ser significativos o no;
- Si los suscriptores pueden ser anónimos o utilizar pseudónimos;
- Reglas para la interpretación de varios formatos de nombre;

6.1.1. Tipos de Nombres

Los Certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. contienen el nombre distintivo (DN) del emisor y el del solicitante del Certificado en los campos Nombre Emisor (issuer name) y Nombre de Sujeto (subject name).

El nombre distintivo (DN) de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. mínimo contempla los siguientes valores:

Nombre distintivo (DN) de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

CN	Autoridad Certificadora de SeguriData Privada S.A. de C.V.
O	SeguriData Privada S.A. de C.V.
OU	Prestación de Servicios de Certificación
C	MX
S	Distrito Federal
L	Alvaro Obregón
PostalCode	01000

El nombre distintivo (DN) del Nombre de Sujeto contempla los siguientes valores:

Nombre distintivo (DN) Certificado del sujeto	
CN	<APELLIDO1> <APELLIDO2> <NOMBRES>
O	<ORGANIZACION>
OU	<AREA A LA QUE PERTENECE>
C	MX
SN	CURP TITULAR DEL CERTIFICADO
X.500uniqueIdentifier (2.5.4.45)	RFC TITULAR DEL CERTIFICADO

6.1.2. Necesidad de que los Nombres Sean Significativos

Los Certificados emitidos a las entidades finales contienen nombres con semántica comúnmente entendible, lo cual permite la determinación de la identidad del individuo y que para tales efectos viene representada en el campo Nombre de Sujeto dentro del Certificado.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no permite que los suscriptores hagan uso de pseudónimos, es decir, que no sea su verdadero nombre personal el que utilicen para efectos de solicitar un Certificado.

El Certificado de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. contiene el nombre distintivo (DN) con semántica comúnmente entendible que permite la determinación de la identidad de la Autoridad Certificadora con el suscriptor o con el tercero que confía en dicho Certificado.

6.1.3. Reglas para Interpretar Varios Formatos de Nombres

Las reglas utilizadas por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. para interpretar los nombres distintivos (DN) de los titulares o suscriptores de certificados digital cumplen con los estándares internacionales ISO/IEC 9594-8 y el RFC 3280.

Asimismo cumplen con lo que marca la ITFEA en su Anexo F6: “Estándares y Estructura del Certificado”, por lo tanto todos los Certificados emitidos utilizan la codificación UTF8String para los atributos DirectoryString de los campos Emisor y Nombre de Sujeto, mientras que la codificación para los campos país (C) y número de serie (SN) es PrintableString.

6.1.4. Unicidad de los Nombres

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. asegura que los nombres distintivos (DN) del Nombre de Sujeto del suscriptor son únicos dentro del dominio, al utilizar la CURP mediante el uso de componentes automatizados en el proceso de inscripción del suscriptor garantizan la unicidad del nombre distintivo (DN).

6.1.5. Procedimiento de Resolución de Conflictos sobre Nombres

Será responsabilidad de los solicitantes de Certificados el cerciorarse de que el nombre que están utilizando en el apartado Nombre de Sujeto de su Certificado no infringe los derechos de propiedad intelectual de otros solicitantes, así pues la Autoridad Certificadora de SeguriData Privada S.A. de C.V. no realizará dicha verificación con alguna institución de Gobierno, ni resolverá cualquier disputa sobre propiedad intelectual del nombre.

En caso de que existiera alguna disputa relacionada con el uso del nombre de los solicitantes, la Autoridad Certificadora de SeguriData Privada S.A. de C.V. y sin alguna responsabilidad hacia cualquier solicitante o suscriptor de Certificados, tendrá la facultad de rechazar la solicitud o revocar el Certificado debido a tal disputa.

6.1.6. Reconocimiento, Autenticación y Papel de Marcas Registradas

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no emitirá Certificados a solicitantes que hayan usado deliberadamente un nombre cuyo derecho de uso no es de su propiedad, asimismo la Autoridad Certificadora no verificará con alguna institución de Gobierno la posesión del nombre o marca registrada en el proceso de Certificación.

6.2. Validación de la Identificación Inicial

Este subcomponente contiene los elementos para los procedimientos de identificación y autenticación del registro inicial para cada tipo de usuario (Agente Certificador o suscriptor):

- Cómo el usuario debe demostrar la posesión de los Datos de Creación de Firma electrónica avanzada con respecto a la correspondiente clave pública que se registra.
- Requisitos de identificación y autenticación para un suscriptor individual o una persona que actúe en nombre de una organización, incluyendo:
    - Tipo de documentación y/o número de identificación (credencial) necesarias (identificación oficial IFE o INE, o pasaporte, o cedula profesional, comprobante de domicilio, CURP para personas físicas nacionalidad mexicana, FM2 o FM3 para extranjeros residentes temporales o permanentes en México, y pasaporte para extranjeros sin residencia en México.
    - Cómo un Agente Certificador autentica la identidad de la persona física nacionalidad mexicana o extranjeros, del representante legal de la persona moral, basándose en la documentación o credenciales proporcionadas;
    - Si el individuo debe presentarse personalmente a la autenticación con el Agente Certificador;
    - Cómo un individuo que representa a una persona moral es autenticado, a través del representante legal de la persona moral.

6.2.1. Método para Probar la Posesión de los Datos de Creación de Firma electrónica avanzada

La posesión de los datos de creación de Firma electrónica avanzada del suscriptor se prueba mediante el requerimiento PKCS10, de manera que si la firma es válida, el suscriptor está en posesión de la llave privada.

6.2.2. Autenticación de la Identidad de un Individuo

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. recaba una serie de documentos para realizar una correcta verificación de la identidad del solicitante de Certificado, esto bajo consentimiento explícito y conforme a lo que señala la Política de Certificados; por lo tanto, en caso de que se trate de una primera inscripción, el solicitante deberá acudir con el Agente Certificador. El trámite es personal e intransferible por lo que el interesado deberá presentarse en las instalaciones para realizarlo.

Los documentos a presentar para la obtención del Certificado son:

- Identificación Oficial Vigente (IFE o INE , o pasaporte o Cedula profesional)
- Clave Única de Registro de Población o Cédula del Registro Federal de Contribuyentes, para personas físicas con nacionalidad mexicana
- FM2 o FM3 para personas extranjeras con residencia temporal o permanente en México
- Pasaporte para personas extranjeras no residentes en México
- Comprobante de Domicilio actual

6.2.3. Autenticación de la Identidad de una Organización Mexicana o Extranjera

La autenticación de la Identidad de una Organización será mediante el Apoderado Legal o la persona con suficiente poder, que represente a la organización que busca obtener su Certificado.

La persona que representa a la organización deberá acudir con el Agente Certificador con una serie de documentos para solicitar su Certificado, los cuales son:

- Acta Constitutiva
- Reformas a la Escritura Constitutiva
- Poder notarial del Apoderado Legal

- Identificación oficial vigente del Apoderado Legal
- Cédula del Registro Federal de Contribuyentes del Apoderado Legal
- Comprobante de domicilio actual del Apoderado Legal
- Cédula del Registro Federal de Contribuyentes de la Persona Moral
- Comprobante de domicilio actual de la organización

Para empresas extranjeras:

- Acta constitutiva , apostillada y traducida al español
- Poder del representante legal o persona con facultades para actos de administración , apostillada y traducida al español
- Documento de impuestos en el país de origen
- Comprobante de domicilio de la organización del país de origen

6.2.4. Autenticación de la Identidad de un Agente Certificador

La autenticación de la identidad de un Agente Certificador se llevará a cabo por el Profesional Jurídico y podría apoyarse con el Oficial de Seguridad, para la emisión del Certificado.

La documentación a presentar por parte del solicitante de Agente Certificador para el caso de que se trate de una persona física, es:

- Identificación Oficial Vigente (IFE o INE, o pasaporte o Cedula profesional)
- Clave Única de Registro de Población o Registro Federal de Contribuyentes para personas físicas con nacionalidad mexicana
- Comprobante de domicilio actual

La documentación a presentar por parte del solicitante de Agente Certificador para el caso de que se trate de una Organización, será mediante el Apoderado Legal o la persona con suficiente poder, que represente a la organización que busca obtener su Certificado.

La persona que representa a la organización deberá acudir con:

- Acta Constitutiva
- Reformas a la Escritura Constitutiva

- Poder notarial del Apoderado Legal
- Identificación oficial vigente del Apoderado Legal
- Cédula del Registro Federal de Contribuyentes del Apoderado Legal
- Comprobante de domicilio actual del Apoderado Legal
- Cédula del Registro Federal de Contribuyentes de la Persona Moral
- Comprobante de domicilio actual de la organización

6.2.5. Solicitudes de Renovación de Llaves

Se requiere que todos los titulares de un Certificado emitido por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. Renueven sus Certificados, antes de su vencimiento, hasta dos semanas antes, con el fin de mantener su continuidad en el uso de su Certificado para Firma electrónica avanzada.

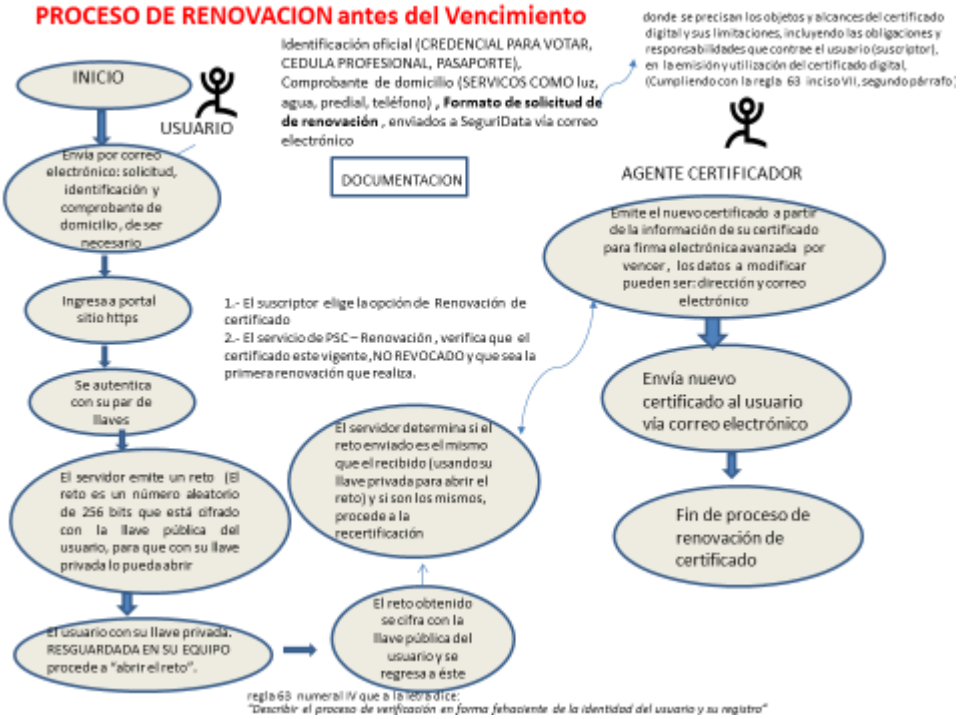
La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que el titular ingrese al portal de PSC SeguriData a la opción de Renovación de certificados. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. para la Renovación de un certificado, define las siguientes políticas:

1.- El certificado para firma electrónica avanzada, debe estar vigente y no revocado, al momento de renovar, esta validación la realiza PSC SeguriData al momento en que el cliente accede al portal. En caso de que el certificado este vencido, debe realizar la emisión de un nuevo certificado de manera presencial.

2.- La persona que realiza la renovación debe ser el propietario del certificado para firma electrónica avanzada y poseer la llave privada, la llave pública y el password asociado

3.- Las llaves para firma electrónica avanzada a renovar deben estar instaladas en el browser del usuario, para ingresar a un sitio seguro protocolo https, cabe mencionar que la llave privada siempre está con el cliente.

4.- La renovación del certificado digital, para firma electrónica avanzada, se puede realizar únicamente en una ocasión antes de su vencimiento, para el siguiente vencimiento, será necesario realizar la validación de la personalidad del propietario, de manera presencial.



La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que el titular ingrese al portal de PSC SeguriData con protocolo https a la opción de Renovación de certificados. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. para la Renovación de un certificado, define el siguiente proceso:

Prerrequisitos:

Enviar por correo electrónico al agente certificador, el mismo día en que realiza la renovación, la siguiente documentación, firmada de manera autógrafa:

1) Solicitud de renovación, donde se precisan los objetos y alcances del certificado digital y sus limitaciones, incluyendo las obligaciones y responsabilidades que contrae el usuario (suscriptor), en la emisión y utilización del certificado digital
2) Copia de identificación oficial (INE O IFE,O PASAPORTE O CEDULA PROFESIONAL)
3) Copia de comprobante de domicilio , en caso de que se actualice

1.- El cliente procede a ingresar al portal de SeguriData PSC con protocolo https, opción renovar par de llaves

El sitio al que ingresa el suscriptor para realizar la renovación de sus llaves es del tipo canal seguro https con autenticación de cliente. De esta forma es la única manera en la que se asegura que no hay nadie en el medio que pudiera interceptar la comunicación.

Para acceder al sitio https, el suscriptor debe instalar el certificado y la llave privada en el browser de su equipo, al ingresar con protocolo https, se tiene la autenticación del dueño del certificado, cumpliendo así con la verificación en forma fehaciente de la identidad del usuario y su registro.

La aplicación valida los prerrequisitos a cumplir para la renovación del certificado

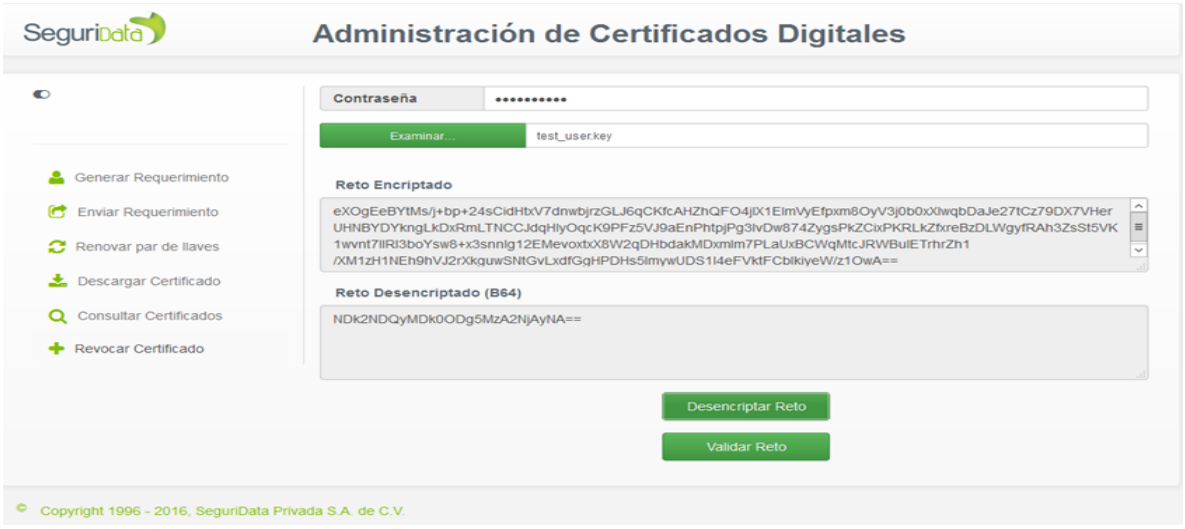
a) Contra OCSP que el certificado no este revocado
b) Contra fecha de vencimiento de certificado que cumpla la condición de hasta 2 semanas antes de su vencimiento
c) Que no se halla renovado anteriormente

Con esto se cubre el numeral VII de la regla 63

"Definir el procedimiento para la renovación del certificado Digital, pudiéndose llevar acabo de manera alterna entre presencial y vía remota, siempre y cuando el certificado se encuentre vigente. En ningún caso podrá renovarse el certificado Digital de manera remota por más de una ocasión"

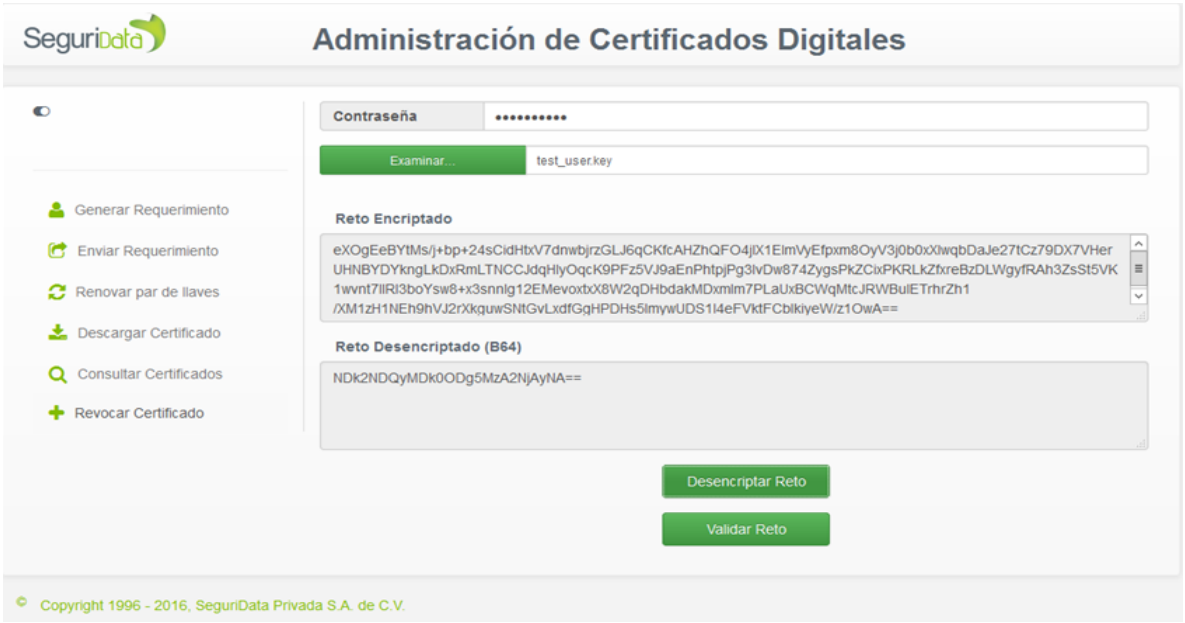
Si se cumplen las condiciones anteriores: Se establece una segunda validación de la autenticación del dueño del certificado a través de:

Paso 1. El servidor genera un reto que se presenta en la pantalla del usuario en base 64.



Paso 2: El usuario debe proveer el certificado, la llave privada y el password de ésta. Con la llave privada se procede a “abrir el reto”.

El reto es un número aleatorio de 256 bits que está cifrado con la llave pública del usuario, para que con su llave privada lo pueda abrir.



Paso 3: El reto obtenido se cifra con la llave pública del servicio y se regresa a éste.

Paso 4. El servidor determina si el reto enviado es el mismo que el recibido (usando su llave privada para abrir el reto) y si son los mismos, procede a la renovación de sus llaves.

Los datos, se toman del certificado actual, los únicos datos a modificar son: la dirección, solo en caso de ser necesario y previo envió del comprobante de domicilio al agente certificador, y el correo electrónico, en caso de no ser actual, puesto que el nuevo certificado sería enviado a dicho correo.

El suscriptor envía el requerimiento, quedando la llave privada en posesión del mismo, en su sistema de archivos, y el agente certificador valida la información y emite el certificado con dos años de vigencia a partir de la fecha en que se emita,

Al momento de emitir el certificado este es enviado automáticamente al correo registrado por el suscriptor.

Existe también la opción de descargar el certificado.

Cabe mencionar que SeguriData nunca tendrá la llave privada del certificado.

Las peticiones cuando las claves de los Certificados ya vencieron, son llevadas a cabo de la misma manera que las peticiones de Certificados nuevos por lo que el usuario realiza el proceso de emisión de certificado tradicional, y valida su personalidad ante el agente certificador de manera presencial.

6.2.6. Solicitudes Emisión de Claves Después de una Revocación

Si un certificado es revocado, puede ser emitido mediante una nueva solicitud

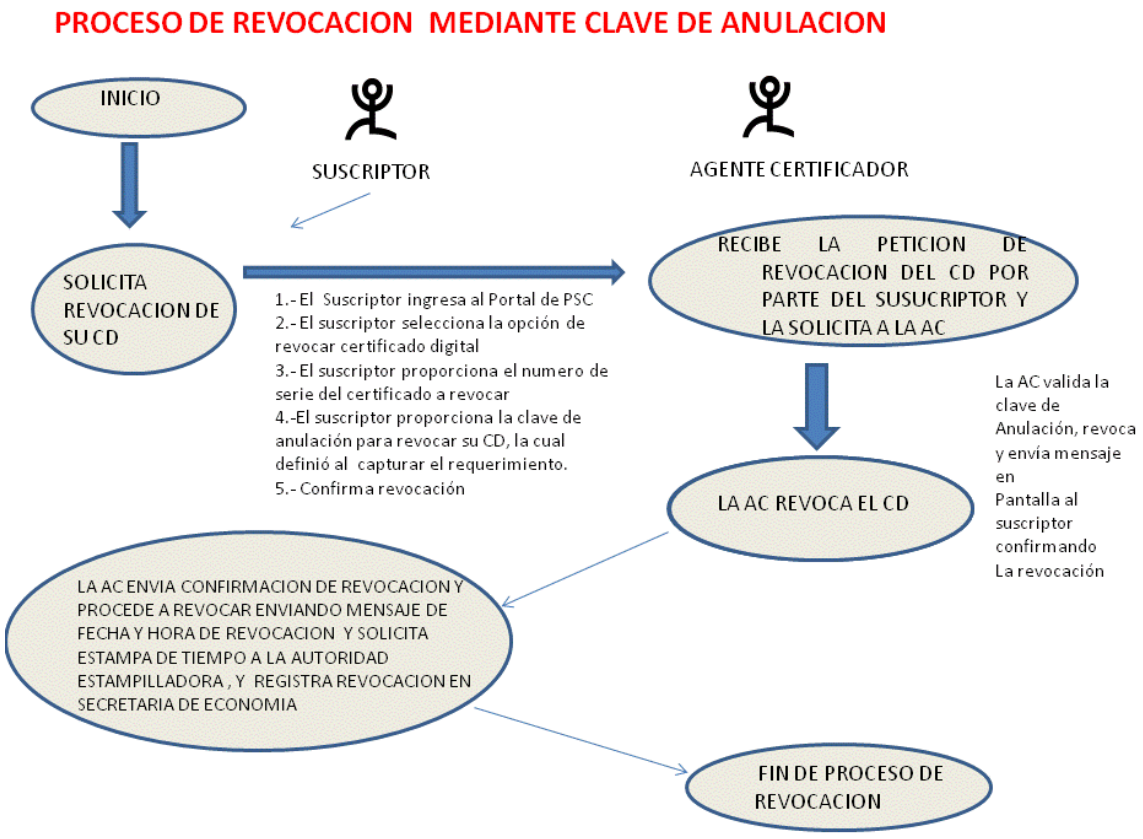
La Autoridad Certificadora de SeguriData Privada S.A. de C.V. se reserva el derecho de negar la emisión del Certificado sí sucede lo siguiente:

- El Certificado fue emitido sin la autorización del individuo nombrado en el campo Nombre de Sujeto.
- Se aplicó la revocación porque el Certificado fue emitido a una persona distinta a la nombrada en el campo Nombre de Sujeto.
- Se descubre que la información proporcionada en la solicitud de Certificado es falsa.

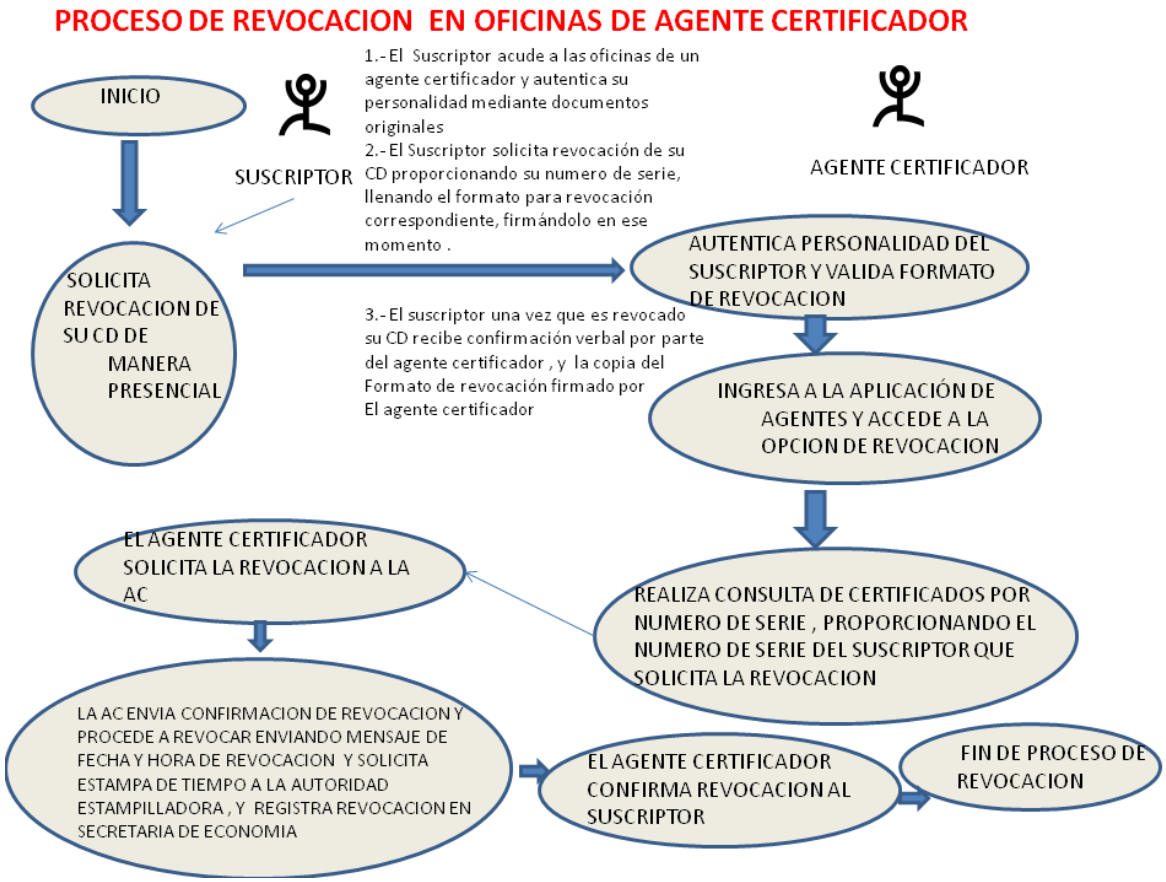
6.3. Identificación y Autenticación para Solicitudes de Revocación

Las solicitudes de revocación se realizarán personalmente por el titular del Certificado mediante los dos métodos dispuestos por la Autoridad Certificadora.

Para el primer método de revocación, el titular del Certificado deberá de comprobar la posesión de los Datos de Creación de Firma electrónica avanzada por medio de la clave de anulación definida durante el proceso de Certificación.



En el segundo método, la Autoridad Certificadora de SeguriData Privada S.A. de C.V. pone a disposición del titular del Certificado oficinas debidamente equipadas para realizar la revocación del Certificado, por lo tanto es necesaria la presencia física del titular acompañado de una solicitud de revocación de Certificado. El usuario suscriptor acudirá presencialmente a las oficinas del Agente Certificador, llevara la Solicitud de Revocación, presentara los documentos que validen su identidad.



La documentación a presentar para llevar a cabo la revocación por el segundo método es:

- Identificación oficial vigente con fotografía. (Credencial del IFE o INE, o pasaporte o Cédula Profesional)

El Agente Certificador, validará los rasgos físicos de la fotografía de la identificación vigente con los rasgos físicos del suscriptor, y en caso de que existiese una controversia para la identificación del suscriptor, se le pediría además los siguientes documentos.

- Comprobante de Domicilio a nombre del suscriptor con la dirección que aparece en los datos que registró para la emisión del certificado.
- CURP impresa.

Una vez aprobada la identidad del suscriptor, este mismo debe llenar la solicitud de revocación y firmarla autógrafamente, para que el Agente Certificador proceda con la solicitud de revocación hacia la Autoridad Certificadora.

7. Ciclo de Vida del Certificado y Exigencias Operacionales

En este componente se especifican los requisitos impuestos a la emisión de Certificados con respecto a su ciclo de vida para Agentes Certificadores, suscriptores o de otros participantes de la Infraestructura de Clave Pública.

7.1. Solicitud de los Certificados

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. se reserva el derecho de rechazar aquellas solicitudes de Certificados que incumplan con algún requisito dispuesto en la presente Política de Certificados.

En caso de que La Autoridad Certificadora haya rechazado la solicitud de Certificado, ésta informará mediante oficio las razones por las que se rechaza dicha solicitud.

7.1.1. Quien puede presentar una Solicitud de Certificado

Una solicitud de Certificado en la forma prescrita por SeguriData Privada S.A. de C.V. debe ser completada por solicitantes, con toda la información de registro tal y como se describe en esta Política de Certificados. Todas las solicitudes están sujetas a revisión, aprobación, y aceptación por parte de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. a su mejor juicio y criterio.

La solicitud de emisión de certificados pueden presentarlas personas físicas de nacionalidad mexicana y extranjeros con residencia temporal o permanente en México, personas físicas con nacionalidad mexicana o extranjeros con residencia en el extranjero que trabajen para empresas mexicanas y representantes legales de personas morales, así como las organizaciones para sus dominios de páginas web para el caso de certificados SSL

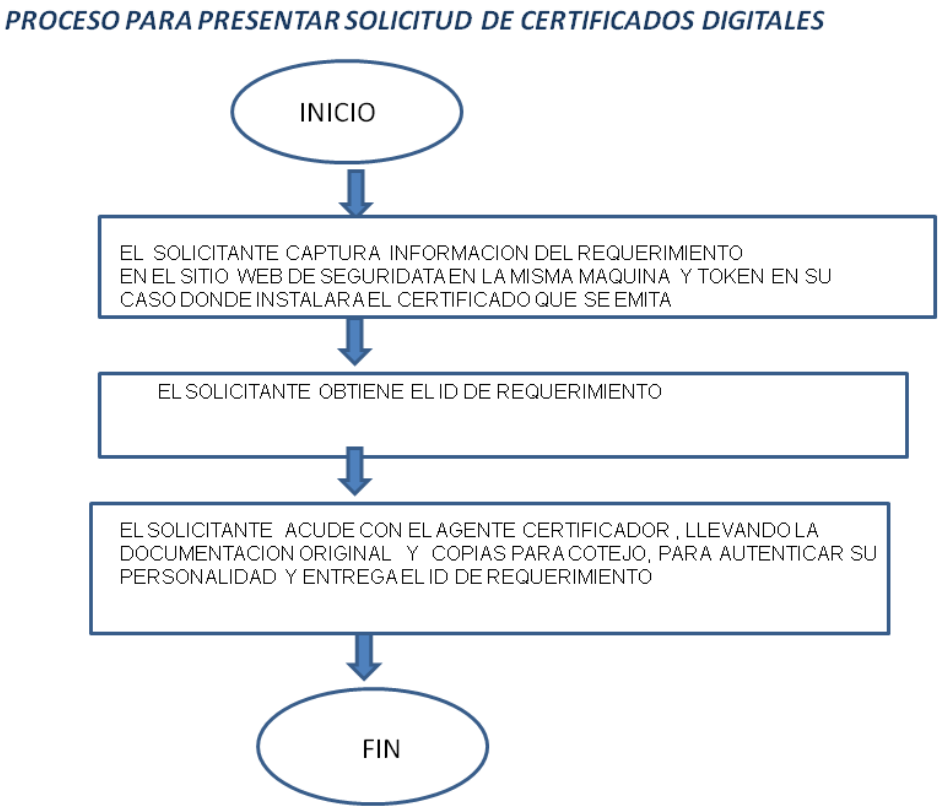
7.1.2. Proceso para Presentar una Solicitud de Certificado

El proceso cubre la parte de generación del par de claves por parte del solicitante, y el envío de la solicitud de Certificado (requerimiento) a la Autoridad Certificadora para que se presente con el Agente Certificador para que este solicite la emisión del Certificado a la Autoridad Certificadora.

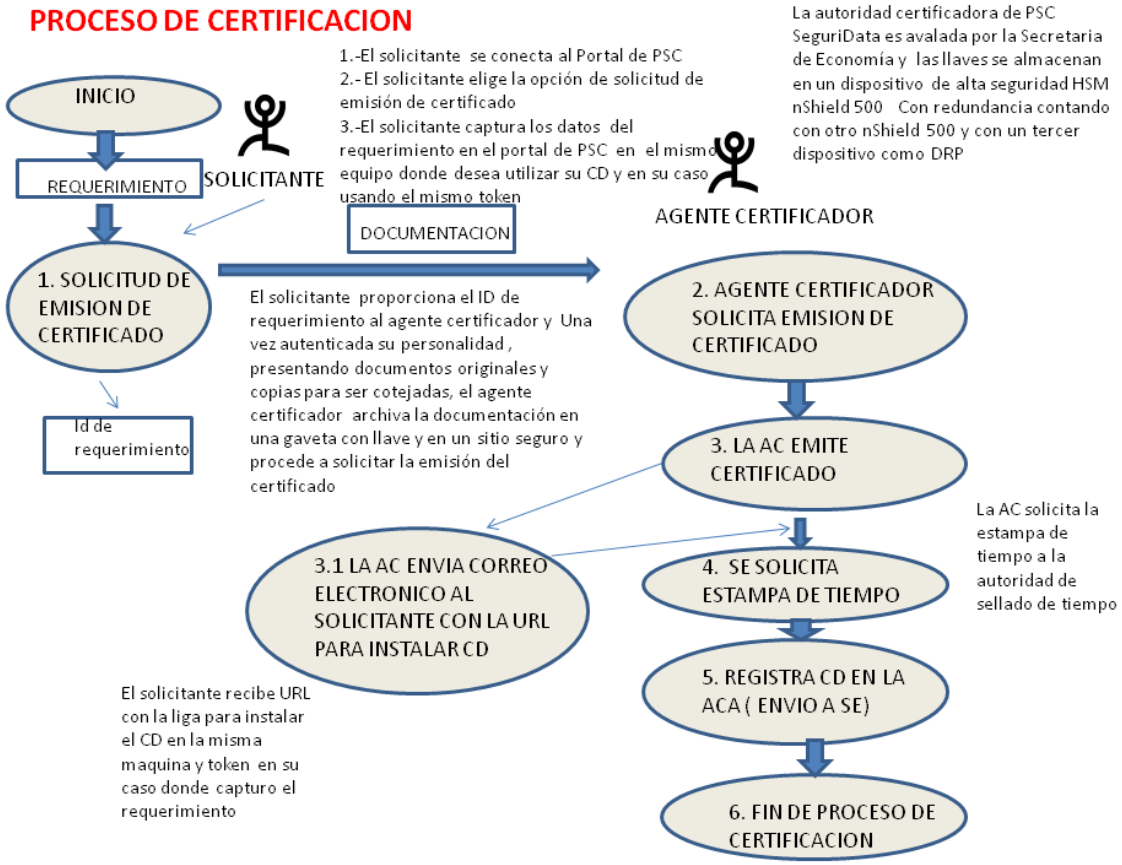
El Agente Certificador tiene la responsabilidad de llevar a cabo el proceso para recibir solicitudes de Certificados.

Asimismo, los solicitantes de Certificados tienen la responsabilidad de proporcionar información precisa en sus solicitudes de Certificado.

A continuación se esquematiza el proceso de enrolamiento:



7.1.3. Descripción del Proceso de Certificación



7.2. Proceso de Solicitud de Certificados

Para obtener un Certificado todos los solicitantes deberán completar el procedimiento de enrolamiento dispuesto por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., la cual incluye las siguientes actividades:

- Generar una cita vía telefónica o correo electrónico con el agente certificador y confirmar su asistencia vía telefónica con al menos 2 días hábiles de anticipación antes de su cita.

- Presentar documentación:

Identificación Oficial (IFE o INE, o pasaporte, o cedula profesional), Id de requerimiento, comprobante de domicilio, CURP y Solicitud de emisión de certificado firmada.

Para el caso de extranjeros en México: FM2 o FM3

Para el caso de extranjeros trabajando para empresas mexicanas en el extranjero: pasaporte, comprobante de domicilio.

El Agente certificador

- Valida los documentos que identifican al solicitante.
- Le da a firmar la solicitud de Certificado, el Acuerdo de Suscriptor y el Aviso de privacidad
- Firmar autógrafamente la Solicitud de Certificado. En caso de que la firma sea de aceptación se continúa con el trámite, en caso de firmarla de rechazo el trámite se cancela.
- Guarda los documentos en una gaveta cerrada con llave en un lugar seguro.
- Certificación:

    1. El Agente Certificador entregara al nuevo suscriptor una copia del Acuerdo de Suscriptor con los datos de la solicitud.

    2. El solicitante recibirá por medio de un correo electrónico la liga donde puede instalar el certificado con la condicionante de que debe ser en el mismo equipo y en su caso token, donde fue capturado el requerimiento.

Para el caso de certificados SSL para sitios web:

1. Generar el CSR en su Servidor Web.
   Una Petición de Firma de Certificado (CSR) es un archivo encriptado que contiene información relacionada con el sitio Web para el cual se está solicitando el Certificado SSL. El mismo es generado en su servidor Web, por lo que el proceso dependerá del servidor Web que usted esté utilizando.

2. Realizar la Solicitud.
   En esta etapa se deberá completar el formulario de Solicitud del Certificado, el cual solicita información relacionada con el solicitante, la empresa y el dominio Web para el cual se está requiriendo el Certificado SSL, además de introducir el archivo CSR.

3. Aceptar la aprobación de solicitud.
   Una vez realizada la Solicitud del Certificado, se consultará en los centros de registros de dominio los datos relacionados con su propietario, mismos que serán validados por PSC SeguriData y se informara al administrador de dominio su aceptación o bien su rechazo.

7.3. Emisión de Certificados

A continuación se describen los elementos relacionados con la emisión del Certificado:

- Acciones realizadas por la Autoridad Certificadora durante la emisión del Certificado
- Mecanismos de notificación por parte de la Autoridad Certificadora hacia los suscriptores de la emisión del Certificado.

7.3.1. Acciones Realizadas por la Autoridad Certificadora Durante la Emisión de los Certificados

Una vez que se da la aprobación definitiva de la solicitud por parte de la Autoridad Certificadora de SeguriData Privada S.A. de C.V., se procede con la emisión segura del Certificado.

Durante la emisión de los Certificados la Autoridad Certificadora de SeguriData Privada S.A. de C.V.:

- Utiliza un procedimiento que vincula de forma segura el Certificado con la información utilizada en la solicitud, también es incluida la clave pública certificada.
- Protege la integridad y confidencialidad de los datos contenidos en la solicitud.
- Solicita la emisión de la estampa de tiempo a la autoridad estampilladora tanto para la emisión como para la revocación de los certificados
- Registra el certificado emitido y la revocación en su caso en la ACA de la Secretaria de Economía.
- Realiza la notificación al suscriptor de la emisión del certificado enviando un correo con la liga de donde puede instalar su certificado en su máquina o en el token que uso en su caso para la captura de su requerimiento

Todos los Certificados iniciarán su vigencia en el momento de su emisión. El periodo de vigencia estará sujeto a una posible extinción anticipada, cuando se den las causas que motiven la revocación del Certificado.

La vigencia de los certificados emitidos para suscriptores no podrá ser superior a 2 años, contados a partir de la fecha en que sean expedidos, de acuerdo al Código de Comercio y por el tamaño de la llave, según las recomendaciones del NIST National Institute of Standards and Technology, basado en la evolución de seguridad en el tamaño de las llaves.

7.3.2. Mecanismos de Notificación de la Autoridad Certificadora al Suscriptor para la entrega del Certificado emitido

.

El solicitante recibirá un correo electrónico que indica la URL para instalar el Certificado, con la condicionante que debe ser en la misma máquina o en su caso token, donde se realizó la captura del requerimiento.

El proceso de instalación del certificado para el suscriptor es

7.4. Registro de Fecha y Hora de la Emisión de Certificados

A lo largo de todo el proceso de certificación, en la base de datos donde se registra la emisión del certificado se tiene la fecha y hora de emisión, la fecha de vencimiento y el número de serie del mismo ,datos que se pueden consultar en el sitio WEB en la consulta del certificado.

7.5. Aceptación de los Certificados

El solicitante deberá de conocer sus derechos y obligaciones que adquiere como titular de un Certificado.

Hasta que la solicitud de emisión de Certificado no sea aceptado, no será emitido.

En caso de aceptar estos derechos y obligaciones el solicitante deberá firmar de manera autógrafa el acuse de recibo que el Agente Certificador le expide; en caso de que no esté de acuerdo, el solicitante deberá expresar su rechazo y firmar de manera autógrafa dicho rechazo.

El solicitante que acepta su Certificado garantiza que toda la información suministrada en relación al proceso de solicitud y toda la información incluida en el Certificado emitido es verdadera y completa. Así como también que ninguna persona no autorizada ha tenido acceso a los Datos de Creación de Firma electrónica avanzada correspondiente al Certificado.

Al término de haber aceptado y firmado de manera autógrafa el acuse de recibo, el titular del Certificado estará listo para participar en procesos electrónicos que requieran su Firma electrónica avanzada, una vez que reciba por correo electrónico la liga para la instalación del mismo.

7.6. Grado de Fiabilidad de los Mecanismos y Dispositivos utilizados

Los puntos importantes para asegurar la fiabilidad de los mecanismos de Firma electrónica avanzada son:

1. La seguridad que se da al acceso a la llave privada tanto de PSC SeguriData como a las de los suscriptores
2. La certeza de tener llaves únicas para PSC SeguriData como para cada uno de los suscriptores
3. La confianza que se tiene en los algoritmos de firma

7.6.1 Seguridad en el acceso a la llave Privada de PSC SeguriData

La llave privada del PSC se encuentra almacenada y custodiada en un módulo HSM que cumple con el FIPS 140-2 nivel 3. Las llaves se generan dentro del módulo y por las características del FIPS 140-2 nivel 3, éstas nunca abandonan el hardware en claro. Incluso, si el hardware fuera manipulado y se abriera, las llaves se eliminarían automáticamente en dicho intento.

La disponibilidad de la llave privada se habilita por medio de un esquema de custodios donde se requiere solo una tarjeta presente de entre 6 tarjetas, para habilitar que el módulo pueda ser usado por el software. El modelo fue seleccionado pensando en la necesidad de alta disponibilidad.

7.6.2 Seguridad en el acceso a la llave Privada del Suscriptor

La seguridad de la llave privada en el caso del suscriptor está dada en algunos de los casos por un token criptográfico que cumple con FIPS 140-2 nivel 2. Las llaves se generan en el módulo y en el caso de intentar extraer las llaves abriéndolo, hay marcas evidentes de que el token ha sido abierto, violando la seguridad del dispositivo.

Existen otros donde no se utiliza un token, en los que la llave privada se almacena en el contenedor del sistema operativo. En dichos casos, la seguridad de la firma digital del suscriptor recae en la seguridad que se imponga en el sistema operativo.

7.6.3 Seguridad en el acceso a la llave privada de los Agentes Certificadores

La llave privada de los agentes certificadores, se encuentran almacenadas y custodiadas en un módulo HSM que cumple con el FIPS 140-2 nivel 3. Las llaves se generan dentro del módulo y por las características del FIPS 140-2 nivel 3, éstas nunca abandonan el hardware en claro. Incluso, si el hardware fuera manipulado y se abriera, las llaves se eliminarían automáticamente en dicho intento.

7.6.4 Certeza de tener llaves únicas para PSC SeguriData

La certeza de poseer llaves únicas para PSC SeguriData está basada en la confianza que se tiene en la calidad de semilla que se genera internamente en el módulo HSM (cumpliendo con FIPS 140-2 nivel3)

7.6.5 Certeza de tener llaves únicas para cada uno de los suscriptores

La certeza de poseer llaves únicas para PSC SeguriData está basada en la confianza que se tiene en la calidad de semilla que se genera internamente en el token junto con el proveedor criptográfico asignado en el sistema operativo.

7.6.6 Confianza en los algoritmos de firma

Con respecto a la confianza que se tiene en los algoritmos de firma utilizados, éstos son algoritmos conocidos públicamente a nivel mundial y tienen aceptación en procesos gubernamentales y de seguridad informática. Son aceptados por gobiernos extranjeros en documentos como el FIPS 186-3 como parte de los principales algoritmos de firma electrónica avanzada.

7.7. Par de Claves y Uso de Certificados

Este subcomponente describe las responsabilidades relacionadas con el uso de claves y certificados, incluyendo:

- Las responsabilidades del suscriptor relativas al uso de los Datos de Creación de Firma electrónica avanzada y Certificado.

7.7.1. Responsabilidades del Suscriptor Relativas al Uso del Certificado y Par de Claves

Dentro de la Infraestructura de Clave Pública un suscriptor sólo puede usar la clave pública y los correspondientes Datos de Creación de Firma electrónica avanzada de un Certificado para los servicios para los que fue emitido el Certificado y una vez que el suscriptor ha aceptado el Acuerdo de Suscriptor. El suscriptor acepta el acuerdo al recibir el Certificado y por lo tanto sin condiciones acuerda usar el Certificado de forma compatible con las aplicaciones listadas a continuación:

1. Firma electrónica avanzada
2. Firma de Correo Electrónico Seguro
3. Firma de Código (aplicaciones)
4. Autenticación de usuarios
5. Certificados SSL para protección de sitios WEB https

a. Modificación de los Certificados

La Infraestructura de Clave Pública de SeguriData Privada S.A. de C.V. no apoya la modificación del Certificado. En caso de requerir cambiar algún dato del certificado, se debe revocar y solicitar la emisión de uno nuevo siguiente el proceso definido para la certificación.

b. Revocación de los Certificados

Para la revocación de los Certificados se abordan los siguientes temas:

- Circunstancias bajo las cuales un Certificado podrá ser revocado;
- Quién puede solicitar la revocación del Certificado del suscriptor;
- Procedimientos utilizados para la solicitud de revocación de Certificado;
- Revisión de la disponibilidad en línea del estado de revocación;
- Otras formas disponibles de anunciar la revocación;

c. Circunstancias de la Revocación de un Certificado

Los Certificados serán revocados cuando cualquier información contenida en ellos se modifica o se hace obsoleta o cuando los Datos de Creación de Firma electrónica avanzada asociados con el Certificado estén o se sospeche que hayan sido comprometidos.

Un Certificado será revocado en los siguientes casos tras la notificación:

- Revelación de las claves del Certificado de la Autoridad Certificadora.
- El suscriptor ha incumplido sus obligaciones bajo esta Política de Certificados o cualquier otro acuerdo;
- Cuando el suscriptor o el Agente Certificador solicitan la revocación por:
    - Solicitud expresa del suscriptor.
    - Incapacidad jurídica declarada por una autoridad competente.
    - Resolución judicial.

- Información falsa o incorrecta contenida en el Certificado.
- Por duplicidad de los Datos de Creación de Firma electrónica avanzada correspondientes al Certificado.
- Muerte del suscriptor.
- Incumplimiento por parte del suscriptor de sus obligaciones, previa notificación por parte del Agente Certificador especificando la causa, fecha y hora en que tendrá efecto la revocación del Certificado.

En el Caso de que la Autoridad Certificadora determinase que sus Certificados podrían verse comprometidos y que la revocación de Certificados es útil para los intereses de la Infraestructura de Clave Pública, después de poner el remedio necesario, SeguriData Privada S.A. de C.V. hará todos los esfuerzos posibles para aprobar la nueva emisión de Certificados a usuarios cuanto antes, a no ser que las acciones de los usuarios estuvieran incumpliendo la Declaración de Prácticas de Certificación, la Política de Certificados u otros documentos contractuales.

d. Quien Puede Solicitar la Revocación

Las entidades siguientes pueden solicitar la revocación de un Certificado:

- La Autoridad Certificadora de SeguriData Privada S.A. de C.V.: La Autoridad Certificadora puede revocar cualquier Certificado emitido dentro de la Infraestructura de Clave Pública a su propio juicio y criterio, y publicará la lista de Certificados revocados a través del servicio público OCSP.
- Agentes Certificadores: Cualquier Agente Certificador que funciona dentro de la Infraestructura de Clave Pública puede solicitar la revocación de los Certificados que solicitó para su emisión.
- Titular del Certificado: Un suscriptor dentro de la Infraestructura de Clave Pública puede solicitar la revocación de su Certificado.

e. Procedimiento para Petición de Revocación del Certificado

Un Certificado puede ser revocado por:

- Asistencia en persona del suscriptor ante el Agente Certificador aportando prueba fehaciente de Identificación.

- Utilización del sistema de revocación vía web. El Certificado sólo será revocado con la clave de anulación en poder del suscriptor

f. Período de Gracia de Petición de Revocación del Certificado

No se permite ningún período de gracia una vez que una petición de revocación ha sido verificada. La Autoridad Certificadora revocará los Certificados en cuanto se haya verificado la revocación solicitada.

Las peticiones e informes que se relacionan con la revocación (por ejemplo, debido a la revelación sustancial de los Datos de Creación de Firma electrónica avanzada, la muerte inesperada de un suscriptor o la violación de obligaciones contractuales) serán procesados al tiempo de su recepción, siempre que se realicen por la opción de presentarse directamente con algún agente certificador, en caso de realizarse a través del sitio WEB, la información no se tiene disponible.

g. Tiempo en el Cual la Autoridad Certificadora Debe Tratar la Petición de Revocación del Certificado

La Autoridad Certificadora debe revocar el Certificado dentro de las 24 horas siguientes a la recepción de una petición de revocación válida, siempre que se realice a través de presentarse con el agente certificador, para el caso de que se realice por el Sitio WEB, es en línea, es decir de manera inmediata una vez proporcionada la clave de anulación.

h. Frecuencia de Emisión de las Listas de Certificados Revocados

La lista de Revocación de Certificados se actualiza en intervalos de 24 horas, los 365 días del año, y siempre esta disponible en el Sitio WEB. En la consulta de estatus de certificados.

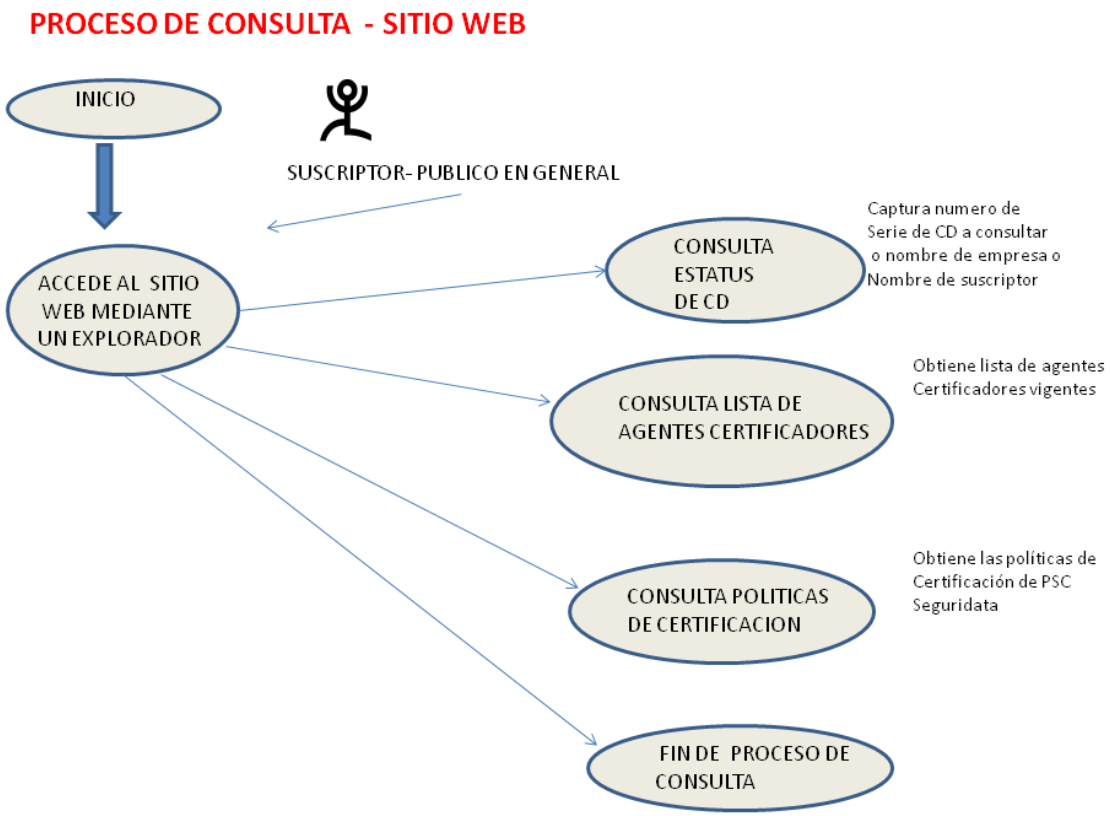
i. Comprobación de la Disponibilidad de la Revocación/Estado en Línea (OCSP)

La información de revocación de los Certificados se proporcionará mediante un servicio de OCSP, 24 horas al día, los 365 días al año, como se especifica en la Política de Certificados.

En caso de fallo del sistema, u otros factores que no sean del control de SeguriData Privada S.A. de C.V., ésta hará todos los esfuerzos posibles para asegurar que este servicio no esté indisponible más del período máximo de tiempo que se especifica en la Declaración de Prácticas de Certificación.

La integridad y la autenticidad de la información del estado de revocación de los Certificados serán protegidas.

La información de estado de revocación será públicamente e internacionalmente disponible, a través de la consulta del estatus de certificados en el Sitio WEB.



j. Comprobación de los Requisitos de la Revocación en línea

La información de revocación de Certificado es proporcionada mediante CRL u OCSP como se especifica en la Política de Certificados.

k. Otras Formas de Publicación de la Revocación Disponible

No se establecen otras formas de Publicación de Revocación disponible.

l. Renovación de certificados

Se requiere que todos los titulares de un Certificado emitido por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. Renueven sus Certificados, antes de su vencimiento, hasta dos semanas antes, con el fin de mantener su continuidad en el uso de su Certificado para Firma electrónica avanzada.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que el titular ingrese al portal de PSC SeguriData a la opción de Renovación de certificados. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. para la Renovación de un certificado, define las siguientes políticas:

1.- El certificado para firma electrónica avanzada, debe estar vigente y no revocado, al momento de renovar, esta validación la realiza PSC SeguriData al momento en que el cliente accede al portal. En caso de que el certificado este vencido, debe realizar la emisión de un nuevo certificado de manera presencial.

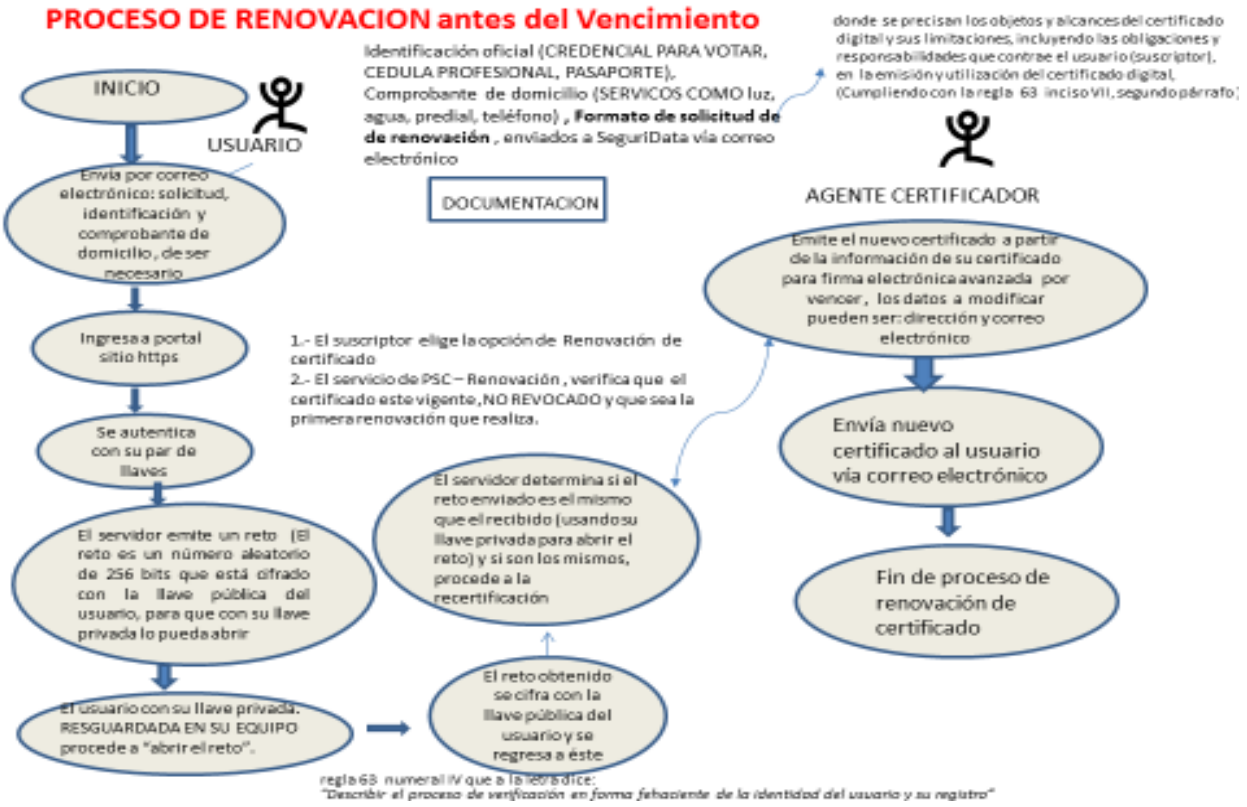
2.- La persona que realiza la renovación debe ser el propietario del certificado para firma electrónica avanzada y poseer la llave privada, la llave pública y el password asociado

3.- Las llaves para firma electrónica avanzada a renovar deben estar instaladas en el browser del usuario, para ingresar a un sitio seguro protocolo https, cabe mencionar que la llave privada siempre está con el cliente.

4.- La renovación del certificado digital, para firma electrónica avanzada, se puede realizar únicamente en una ocasión antes de su vencimiento, para el siguiente vencimiento, será necesario realizar la validación de la personalidad del propietario, de manera presencial.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que el titular ingrese al portal de PSC SeguriData con protocolo https a la opción de Renovación de certificados. La

Autoridad Certificadora de SeguriData Privada S.A. de C.V. para la Renovación de un certificado, define el siguiente procedimiento:



m. Renovación de certificados después de su vencimiento

No es posible la renovación de un certificado después o hasta 2 semanas antes de su vencimiento, si este es el caso, el suscriptor debe realizar la emisión de un certificado nuevo de manera presencial.

n. Circunstancias para Proceder a la Suspensión

El estado de suspensión en los Certificados no está estipulado.

o. Servicio de Consulta del Estado del Certificado

El servicio de comprobación del estado de los Certificados disponible incluye:

- Las características operacionales del servicio de comprobación del estado del Certificado;
- La disponibilidad de tal servicio y cualquier política aplicable a la falta de disponibilidad; y
- Los aspectos opcionales de tal servicio.

p. Características Operacionales

El estado de los Certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. se publicará en una Lista de Revocación de Certificados en el Sitio WEB.

q. Disponibilidad del Servicio

El servicio de consulta del estado de los Certificados está disponible 24 horas por día, 7 días por semana, los 365 días del año.

r. Aspectos Opcionales

Sin estipular.

s. Fin de la Suscripción

Dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. un suscriptor puede finalizar una suscripción por:

- Permitir la expiración de su Certificado sin renovarlo.
- Revocar su Certificado sin renovarlo.

t. Depósito de Garantía de Claves y Recuperación

La Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. no apoya el depósito de garantía de las claves.

8.0 Protección de datos y resguardo de información

PSC SeguriData como Autoridad certificadora tiene el compromiso de resguardar y cumplir las disposiciones contenidas en la fracción II del inciso A del Artículo 102, fracción V y VII del Articulo 104 del Código de Comercio, y último párrafo de la fracción III del Artículo 5, fracción VII y VIII del Artículo 27 del Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación sobre la seguridad de la información y confidencialidad de datos personales. Los datos personales, están referidos a la información y documentación, que se utilizan para identificar al solicitante de un Certificado Digital, ya sea como persona física o como persona moral, al igual que el resto de documentación solicitada, ya sea para su emisión o para su revocación o renovación de un certificado digital.

Los datos personales y documentación recabada para la emisión de Certificados Digitales solo serán utilizados por el agente certificador para la solicitud de emisión del Certificado Digital y para integrar el expediente respectivo del suscriptor.

Las Autoridades Certificadora PSC SeguriData conservará en su expediente en físico, copia de la información y documentación proporcionada por el suscriptor, por un plazo de 10 años contados a partir de la emisión del certificado, después de este plazo el expediente del suscriptor que se encuentra resguardado en físico, será destruido sin ningún perjuicio para la Autoridad certificadora PSC Seguridata.