Declaración de Prácticas de Certificación Aplicables a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

OID: 2.16.484.101.10.316.2.5.1.1.1.2.1.3

Versión 1.5

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 al menos una vez al año o cuando se defina la necesidad de actualizarlo. Es necesario que el responsable de éste lo ligue al proceso de Administración de Cambios, de manera que el manejo de versiones se realice de una manera controlada.

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**	**PROCESO DE RENOVACION DE CERTIFICADOS**
1.3	**SEPTIEMBRE 2018**	**AJUSTES POR INCORPORACIÓN DE RENOVACIÓN AUTOMÁTICA DE CERTIFICADOS EN EL PRIMER VENCIMIENTO, Y ACTUALIZACIÓN DE DATOS DE LA AUTORIDAD CERTIFICADORA**
1.4	**30 MARZO 2021**	**ACTUALIZACIÓN DE CALENDARIO DE REVISIÓN**
1.5	**12 JULIO 2024**	**ACTUALIZACIÓN DE CALENDARIO , ACTUALIZACIÓN DE PROTECCIÓN DE DATOS Y RESGUARDO DE EXPEDIENTES, ASÍ COMO DE NORMATIVA Y SITE ALTERNO DE SANTA FE A TULTITLAN**

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 y se actualizará al menos una vez al año para verificar que el contenido sea aplicable y funcional a la Infraestructura de Clave Pública.

FECHAS PROGRAMADAS DE FUTURAS REVISIONES
30-03-2021
30-03-2022
30-03-2023
30-03-2024
30-03-2025

En caso que durante las revisiones programadas, cambié la versión de la presente Declaración de Prácticas de Certificación, seguirá publicada en el Sitio Web https://psc.seguridata.com las versiones revisadas anteriores a las aprobadas.

2. Introducción

El presente documento corresponde a la Declaración de Prácticas de Certificación (CPS por sus siglas en inglés "Certification Practice Statement") que rige a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. como Prestador de Servicios de Certificación (PSC), de acuerdo a las "Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación" publicadas en el Diario Oficial de la Federación el 14 de mayo de 2018.

El conjunto de disposiciones que se cubren en la presente Declaración de Prácticas de Certificación son:

- Introducción, que describe de manera general la intención del documento.
- Obligaciones y Responsabilidades de los Participantes de la Infraestructura de Clave Pública, donde se precisan cuáles son las obligaciones de la Autoridad Certificadora, las responsabilidades de la Autoridad Certificadora para con los suscriptores y partes que confían, las responsabilidades y obligaciones de los Agentes Certificadores y de los suscriptores.
- Publicación y Responsabilidades del Repositorio, donde se describen el repositorio y las responsabilidades en cuanto a la publicación de los Certificados.
- Identificación y Autenticación, que describe como comprobar la identidad del solicitante de un Certificado.
- Ciclo de Vida del Certificado y Exigencias Operacionales, que describe el ciclo de vida del Certificado de un solicitante/suscriptor, desde que es solicitado, emitido, utilizado, revocado o finaliza su vigencia.
- Gestión, Operación y Controles Físicos, que describe todo lo que está alrededor de los controles físicos para procurar la seguridad de la Autoridad Certificadora.
- Controles de Seguridad Técnica, que describe los controles técnicos aplicados sobre la seguridad alrededor de la Autoridad Certificadora.
- Perfiles del Certificado, CRL y Servicio OCSP, que describe la publicación de listas de revocación de Certificados.
- Auditoría de Cumplimiento y Otras Evaluaciones, que describe las auditorías de cumplimiento sobre la Autoridad Certificadora, y las acciones a tomar como consecuencia de los hallazgos y recomendaciones encontradas.

- Otros Asuntos Comerciales y Asuntos Legales, donde se definen aspectos económicos y de carácter legal para las partes involucradas en la Infraestructura de Clave Pública.

La redacción de la presente Declaración de Prácticas de Certificación está basada en lo dispuesto por la IETF (Internet Engineering Task Force) en el documento de referencia RFC (Request For Comments) 3647, denominado como "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework". Asimismo, para el desarrollo de su contenido, se ha 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".

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	Tiene la función de 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;
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.
Mensaje de datos	La información generada, enviada, recibida o archivada por medios electrónicos, ópticos o cualquier otra tecnología.
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
Titular del certificado	Se entenderá a la persona a cuyo favor fue expedido el Certificado
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 extranjero con residencia en el extranjero, 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.

La presente Declaración de Prácticas de Certificación contiene las prácticas que la Autoridad Certificadora lleva a cabo para la operación y administración de la infraestructura, así como los procedimientos que ésta implementa para cumplir con los requerimientos plasmados en el documento de Política de Certificados. Además la Declaración de Prácticas de Certificación incluye todas las actividades que se desarrollan durante la gestión de los Certificados en su ciclo de vida, por lo que sirve de guía para la relación que existe entre la Autoridad Certificadora y sus suscriptores.

Esta Declaración de Prácticas de Certificación 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.

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 gestionan la emisión de los Certificados, así como también la solicitud de 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.

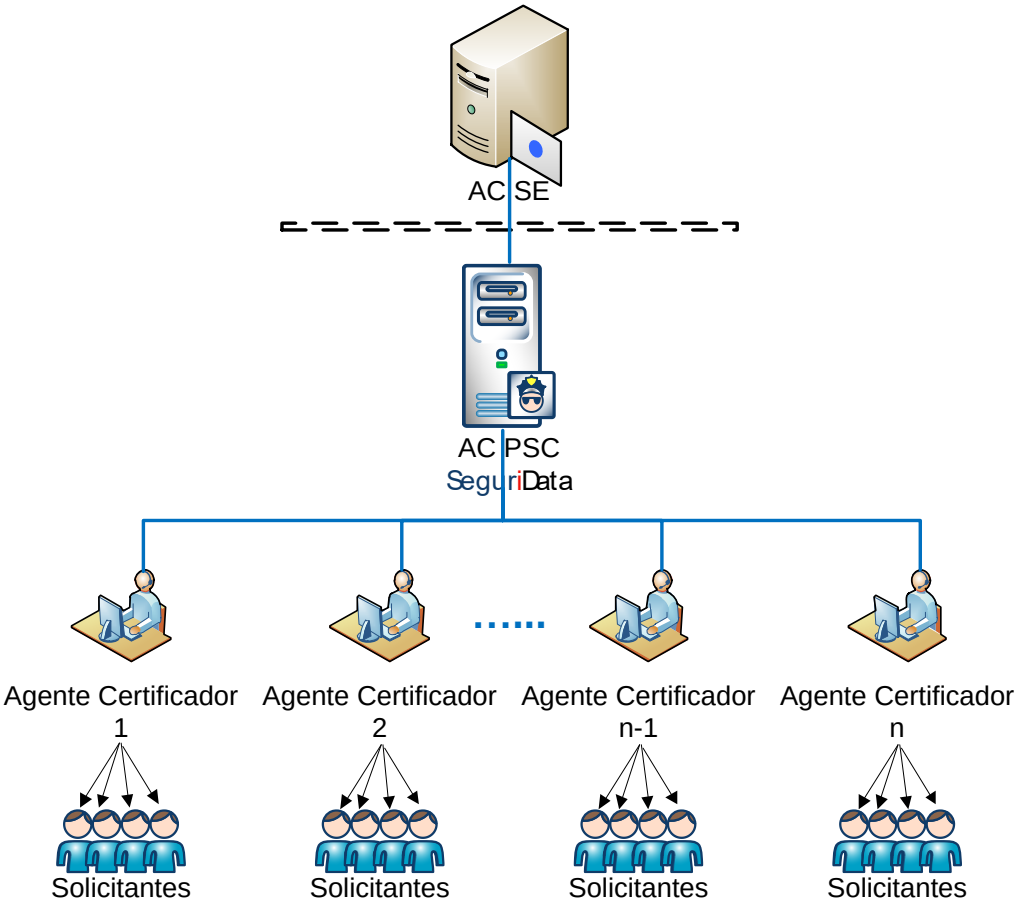


Figura 1

2.3. Nombre del Documento e Identificación

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

Nombre del documento	Declaración de Prácticas de Certificación aplicables a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.
Versión del documento	1.5
Autor	SeguriData Privada S.A. de C.V.
Estado del documento	En autorización por parte de la Secretaría de Economía.
Fecha de emisión	4/04/2011
Fecha de inicio de uso	30/04/2011
Fecha de expiración	No es aplicable
Identificador Digital de Objetos – OID (Object Identifier Digital)	2.16.484.101.10.316.2.5.1.1.1.2.1.3
Localización (URL) de la Declaración de Prácticas de Certificación	https://psc.seguridata.com/docs/doc07.pdf
Ámbito de Aplicación	Ver sección 2.4.

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 (Secretaría de Economía)
- Autoridad Certificadora (PSC)
- Agentes Certificadores llamadas 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 Declaración de Prácticas de Certificación.

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	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 caso de que se incorpore o se realice una baja de una Autoridad Certificadora, se realizará la respectiva modificación a la presente Declaración de Prácticas 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.

Para el inicio de actividades, existirá solamente una oficina destinada para un Agente Certificador, en las oficinas de SeguriData Privada S.A. de C.V. en Insurgentes Sur 2375 Piso 3, Colonia Tizapán, Delegación Álvaro Obregón, en México, Distrito Federal.

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 mismo Distrito federal, a los que llamaremos agentes certificadores externos.

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 expedido 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. Partes que Confían

Las partes que confían son los sujetos o entidades diferentes del titular del Certificado que deciden aceptar y confiar en los Certificados emitidos por la Autoridad Certificadora, así como en las transacciones electrónicas que se lleven a cabo utilizando dichos Certificados.

2.5 Tipos de Certificados que se emiten

Los tipos de Certificados que se emiten 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, previa 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 será de al menos 2 años por el tamaño de la llave, 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 y para los representantes de personas morales.

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
2. Firma de Correo Electrónico Seguro
3. Firma de código (aplicaciones)
4. Autenticación de usuarios (SSL Secure Socket Layer)
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: 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: permite al titular firmar trámites o documentos de manera electrónica. El certificado digital permitirá la sustitución de la firma autógrafa por la firma electrónica con el fin de facilitar y agilizar los actos y negocios jurídicos, comunicaciones y procedimientos administrativos entre las diferentes entidades, particulares y las relaciones que mantengan éstos entre sí. 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.

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.

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 Declaración de Prácticas de Certificación establece.

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 gestionar certificados ante la autoridad certificadora, para firmar otros Certificados, ni para firmar listas de Certificados revocados.

2.6.3 Algoritmos y Parámetros Utilizados

Los Algoritmos de Firma son RSA con digestión Sha-1, los tamaños de claves son de al menos 1024 bits para usuarios y al menos de 2048 bits para Autoridad Certificadora.

2.7 Administración de la Declaración de Prácticas de Certificación

Responsable de la Administración de la Declaración de Prácticas de Certificación	
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

2.7.1 Estructura de los Certificados

El Certificado debe incluir:

1.- La identificación de la AC y el país de donde es.

2.- El nombre del suscriptor.

3.- Los propósitos para los que fue emitido el certificado.

4.-La Clave Publica

5.- El periodo de validez del certificado.

6.- El número de serie del certificado.

7.- La Firma electrónica avanzada de la Autoridad Certificadora emitiendo el certificado.

8.-Limitantes en el uso del certificado, si aplica.

9.-Guía en el periodo de validez.

3 Obligaciones y Responsabilidades de los Participantes de la Infraestructura de Clave Pública

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

3.1 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, 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.

- 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/
- Conservar por medios electrónicos toda la información y documentos relacionados con los Certificados emitidos durante un lapso de al menos 5 años desde su emisión, en particular para verificar las firmas hechas usando los Certificados ya mencionados.
- 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.

3.2 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.

3.3 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 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 bajo la que emiten Certificados...

En consecuencia con estos documentos, las obligaciones de los Agentes Certificadores incluyen, pero no se limitan a:

- 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 oficiales de registro 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 de oficial de registro.

3.4 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.

3.5 Responsabilidades

3.5.1 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 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 avanzada 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.

3.5.2 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.

- 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...

3.5.3 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.

3.6 Limitación de Responsabilidad

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

3.6.1 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 la 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.

3.7 Responsabilidades Económicas

3.7.1 Indemnización por Parte de la Autoridad Certificadora

Estipulado en la sección 12.9 de esta Declaración de Prácticas de Certificación.

3.7.2 Indemnización por Parte de los Suscriptores

Al grado permitido por esta Declaración de Prácticas de Certificación aplicable 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.

4 Publicación y Responsabilidades de Repositorio

4.1 Actualización de la Declaración de Prácticas de Certificación

La última versión autorizada de este documento de Declaración de Prácticas de Certificación 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/docs/doc07.pdf

4.2 Repositorios

SeguriData Privada S.A. de C.V. es responsable de administrar el repositorio de Certificados y Listas de Certificados Revocados (CRL's) de la Autoridad Certificadora.

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.

4.3 Frecuencia de Publicación de CRL y OCSP

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.

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

4.4 Comprobación de la CRL y OCSP

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 mismos contra la última CRL publicada o contra el OCSP de la misma Autoridad Certificadora.

4.4.1 Disponibilidad de la CRL y OCSP

La Autoridad Certificadora ofrece el servicio de consulta en línea de CRL disponible en:

- https://psc.seguridata.com/crl_4096.crl

La Autoridad Certificadora ofrece el servicio de OCSP disponible en:

- http://ocsp.seguridata.com:8083/

4.5 Control de Acceso

La información publicada sobre la Declaración de Prácticas de Certificación, Política de Certificados, OCSP y CRL es de dominio público. Este acceso es de sólo lectura.

5. 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 solicita la renovación de claves antes de su vencimiento y como realizar el proceso de revocación.

5.1 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;

5.2 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	Álvaro 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

5.2.1 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.

5.2.2 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.

5.2.3 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).

5.2.4 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.

5.2.5 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.

5.3 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)

- 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.

5.3.1 Método para Probar la Posesión de los Datos de Creación de Firma electrónica avanzada del suscriptor

La posesión de los datos de creación de firma electrónica 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.

5.3.2 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
- FM2 o FM3 para personas extranjeras con residencia temporal o permanente en México
- Comprobante de Domicilio actual
- Pasaporte para extranjeros

5.3.3 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

5.3.4 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 profesional informático, para la emisión del Certificado.

La documentación a presentar por parte del solicitante de Agente Certificador es:

- Identificación Oficial Vigente (IFE, o pasaporte o Cedula profesional)

- Clave Única de Registro de Población o Registro Federal de Contribuyentes
- Comprobante de domicilio actual

5.3.5 Autenticación para Solicitudes de Renovación de Claves para firma electrónica avanzada en su primer vencimiento

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.

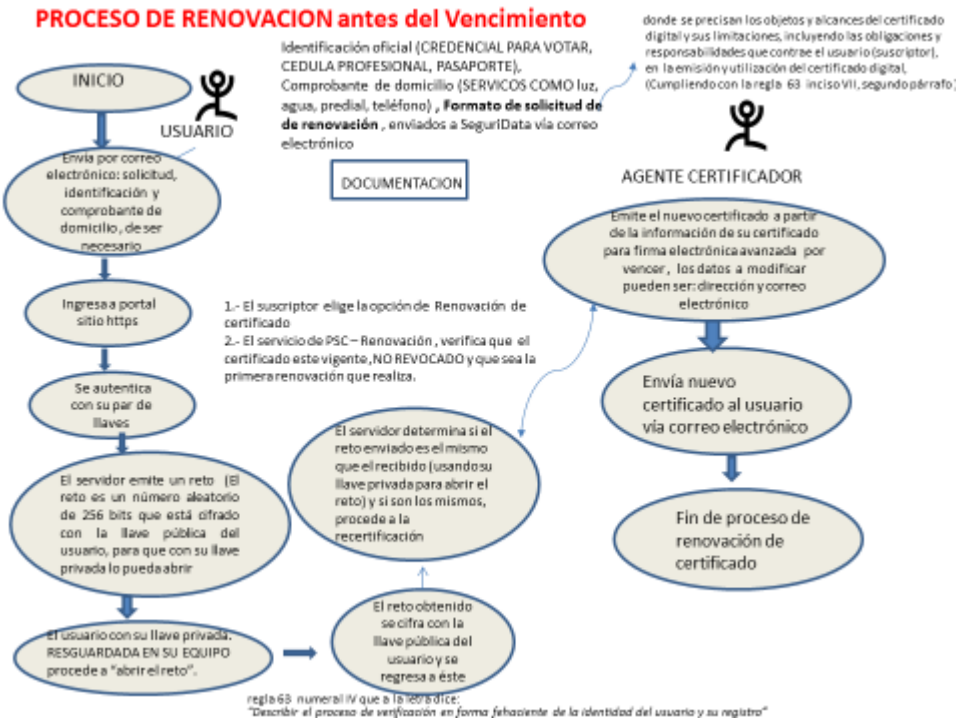
La Autoridad Certificadora de SeguriData Privada S.A. de C.V. requiere que el titular ingrese al portal de PSC SeguriData a la opción de Renovación de certificados. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. para la Renovación de un certificado, define las siguientes políticas:

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

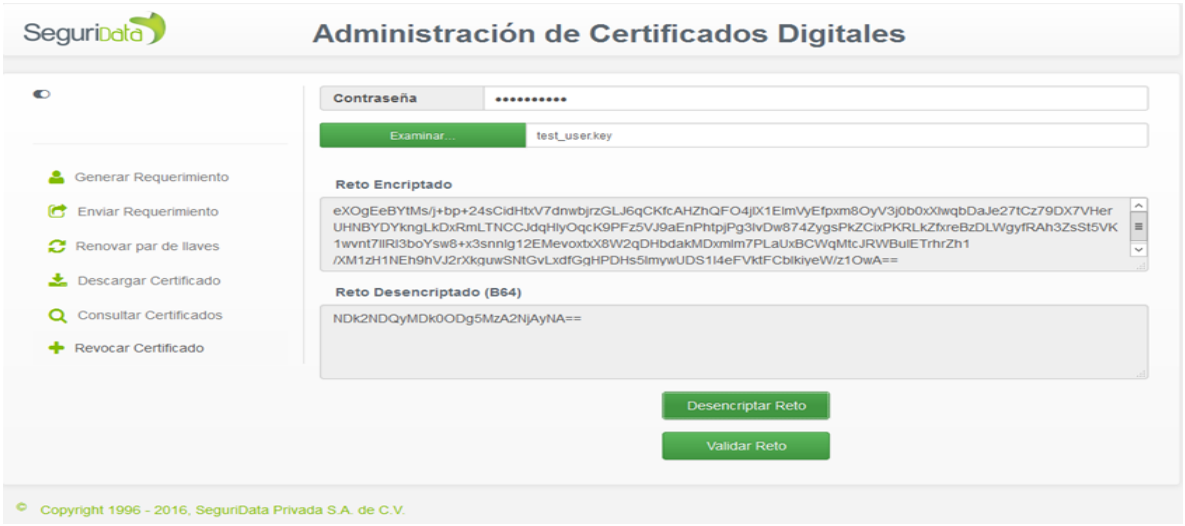
a) Contra OCSP que el certificado no este revocado
b) Contra fecha de vencimiento de certificado que cumpla la condición de hasta 2 semanas antes de su vencimiento
c) Que no se halla renovado anteriormente

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"

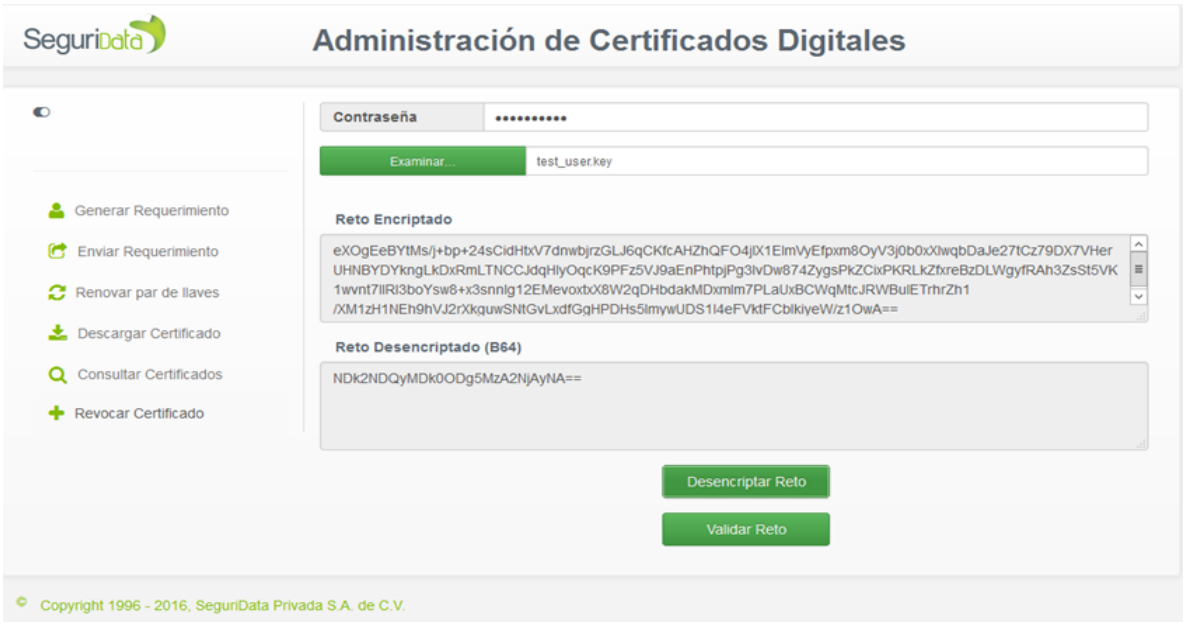
Si se cumplen las condiciones anteriores: Se establece una segunda validación de la autenticación del dueño del certificado a través de:

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.

5.3.6 Solicitudes Emisión de Claves Después de una Revocación

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

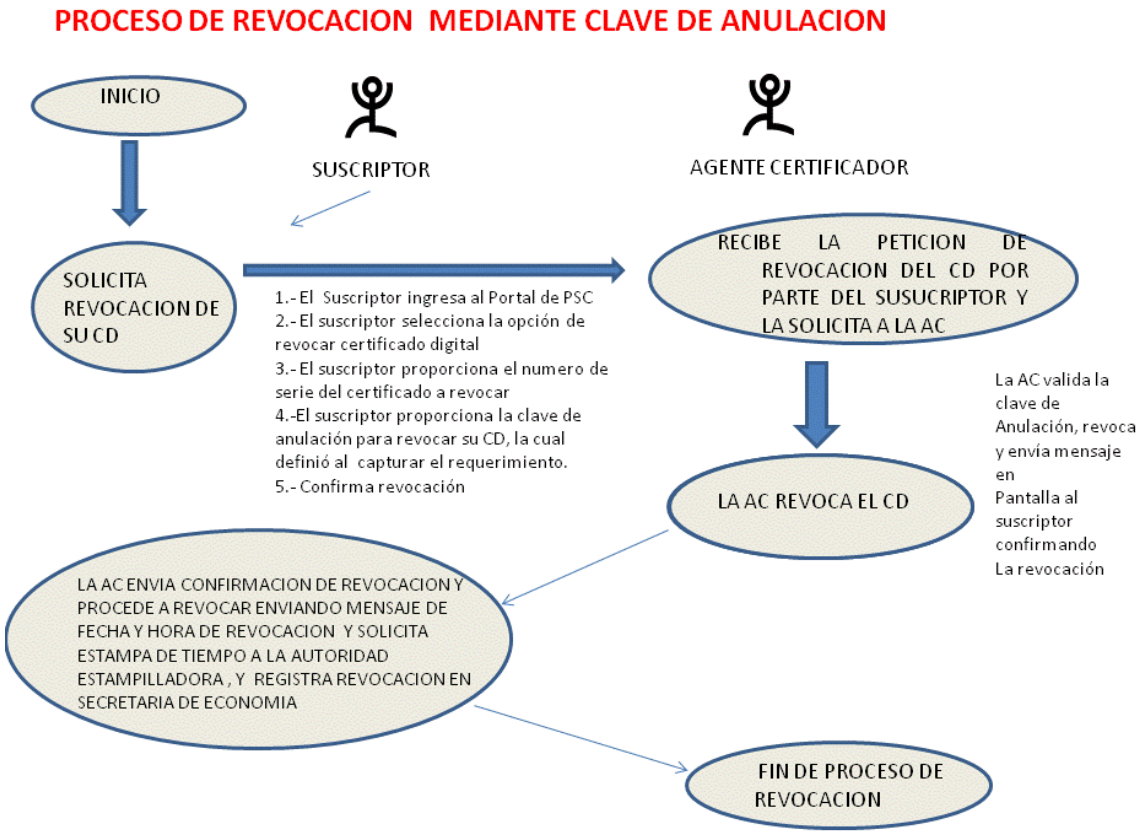
La Autoridad Certificadora de SeguriData Privada S.A. de C.V. se reserva el derecho de negar la emisión del Certificado sí sucede lo siguiente:

- 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.

5.4 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.

6 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.

6.1 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 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.

6.1.1 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 la 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.

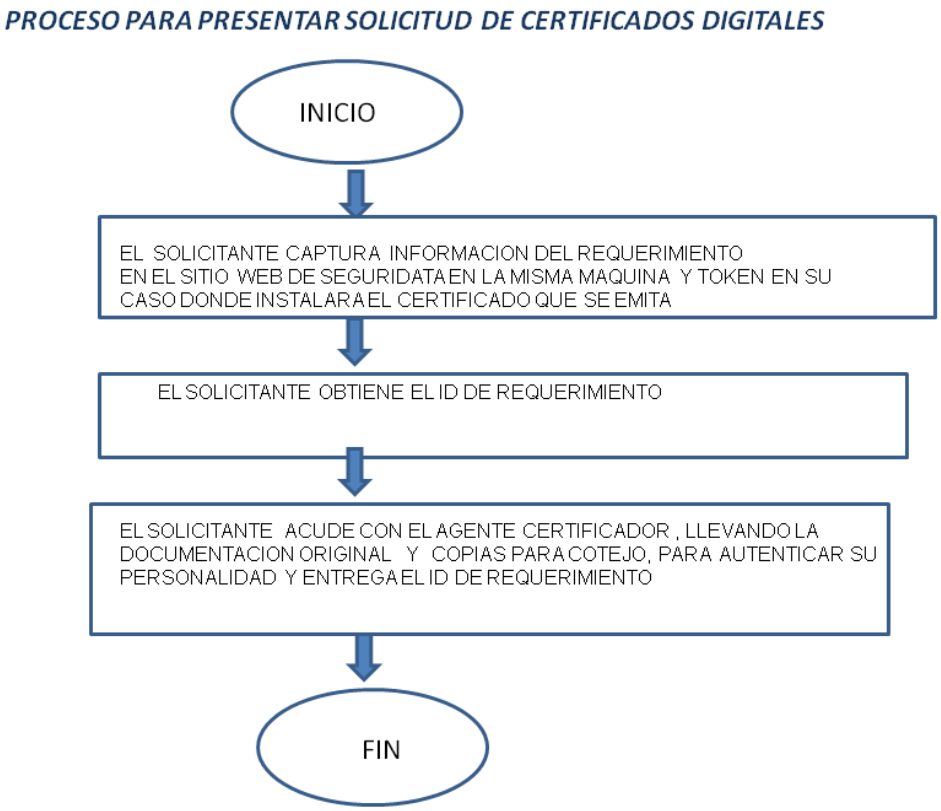
6.1.2 Proceso para Presentar una Solicitud de Certificado

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.

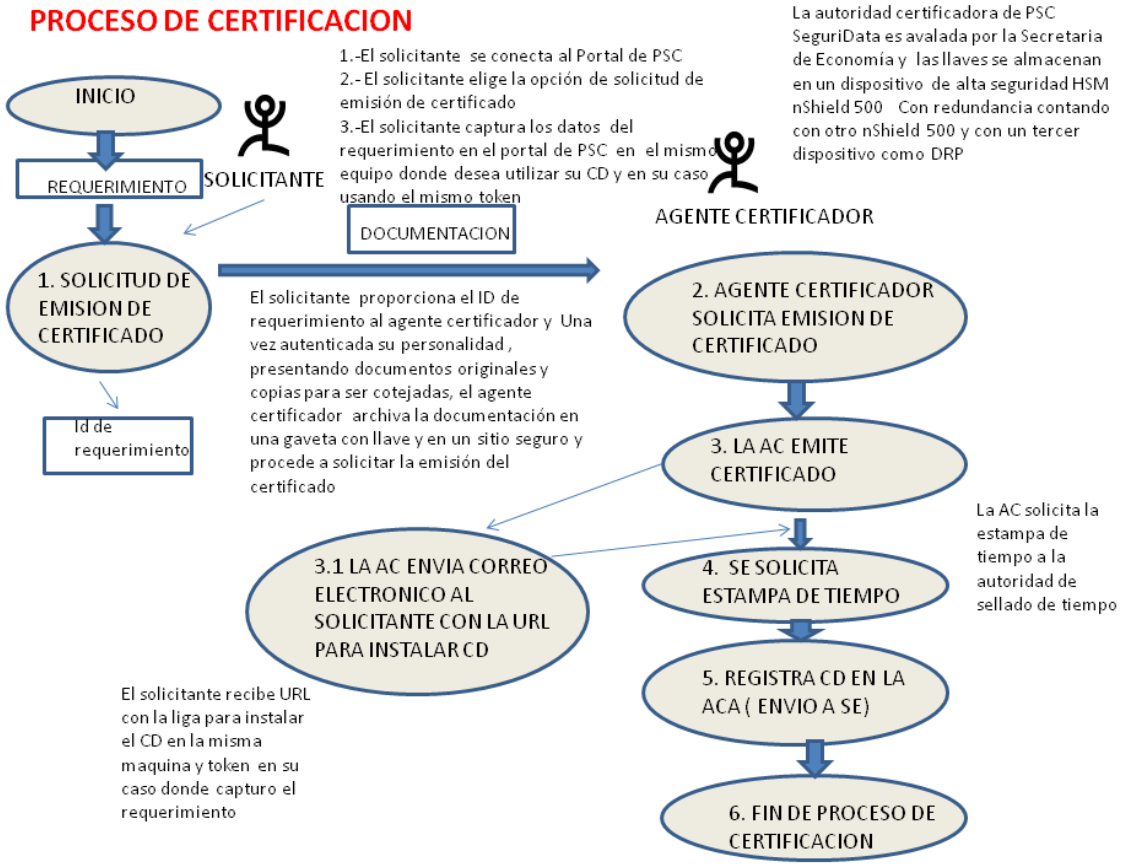
El Agente Certificador tiene la responsabilidad de llevar a cabo el proceso para recibir solicitudes de Certificados.

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

A continuación se esquematiza el proceso para presentar una solicitud de emisión de certificado Digital:



6.1.3 Descripción del Proceso de Certificación



6.2 Proceso de Solicitud de Certificados

Para obtener un Certificado todos los solicitantes deberán completar los procesos definidos 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: Pasaporte

Comprobante de Domicilio

CURP para personas físicas nacionalidad mexicana

El Agente certificador

- Valida los documentos que identifican al solicitante.
- Le da a firmar la solicitud de Certificado, con el Acuerdo de Suscriptor al reverso de la solicitud.
- 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

6.3 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.

6.3.1 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 estampillad ora 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.

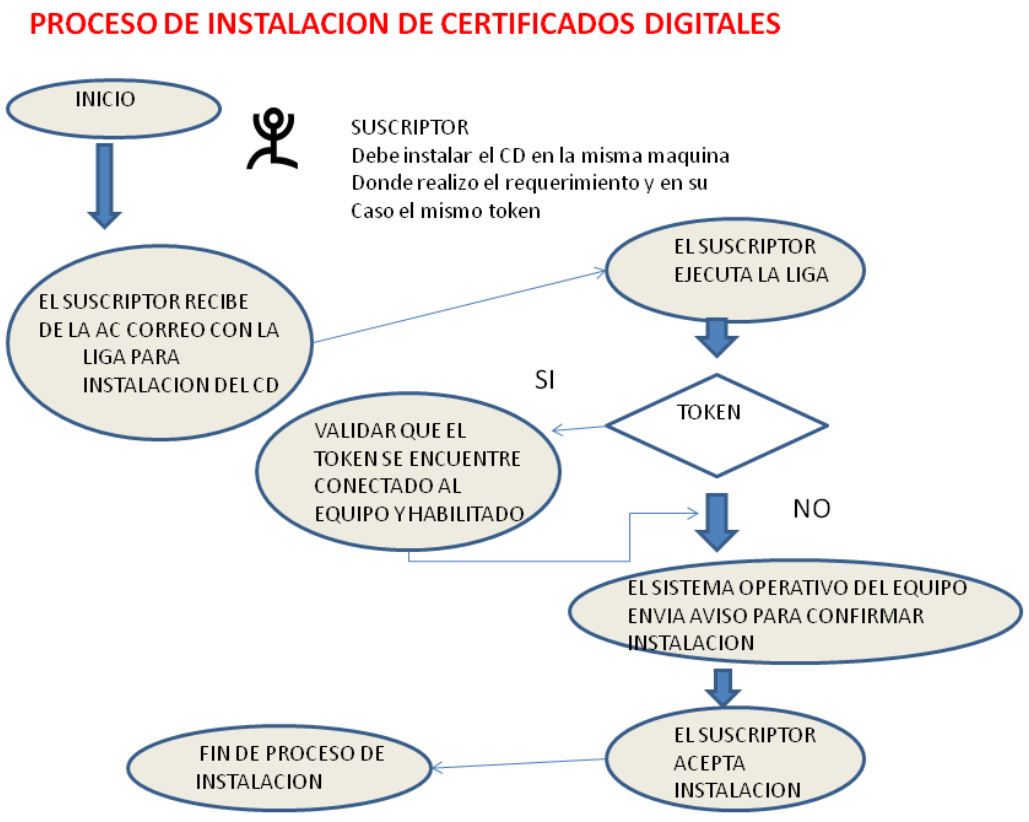
La vigencia de los certificados emitidos para suscriptores es al menos de 2 años por el tamaño de la llave, pero puede variar de acuerdo a las recomendaciones del NIST National Institute of Standards and Technology, basado en la evolución de seguridad en el tamaño de las llaves.

6.3.2 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 realizo la captura del requerimiento.

El proceso de instalación del certificado para el suscriptor es



6.4 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 y datos que se pueden consultar en el Sitio WEB, en la consulta del certificado.

6.5 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, una vez que reciba por correo electrónico la liga para la instalación del mismo.

6.6 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

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.

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.

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)

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.

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 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.

7.1 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
2. Firma de Correo Electrónico Seguro
3. Firma de Código (aplicaciones)
4. Autenticación de usuarios
5. Certificados SSL para protección de sitios WEB https

7.2 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 siguiendo el proceso definido para la certificación.

7.2.1 Quien Puede Solicitar Certificación de una Clave Pública Nueva

Los suscriptores y Agentes Certificadores designados pueden solicitar nuevas claves de Certificados, mediante la solicitud de la emisión de un nuevo certificado

7.3 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;

7.3.1 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.

7.3.2 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 en el Sitio WEB.
- 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.

7.3.3 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 Sitio WEB. El Certificado sólo será revocado con la clave de anulación en poder del suscriptor

7.3.4 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, 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.

7.3.5 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 el suscriptor se presente 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.

7.3.6 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:

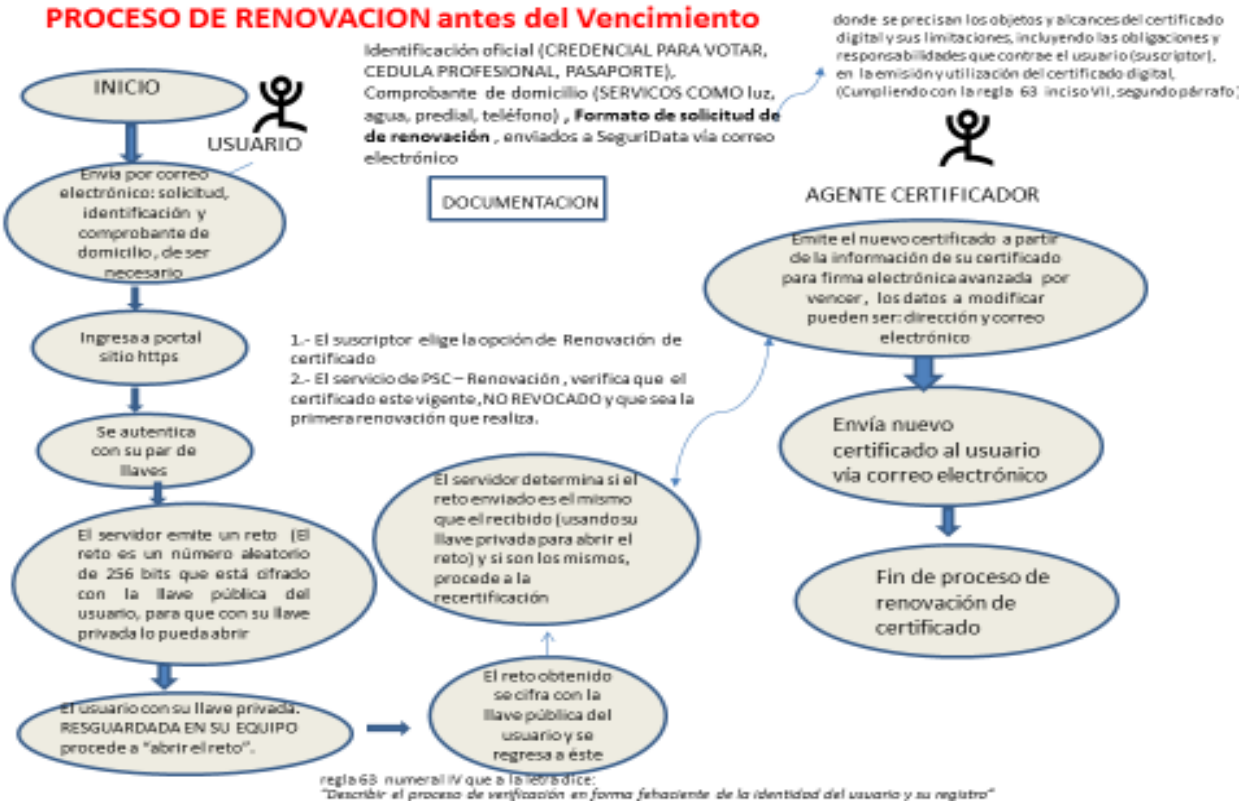
1.- El certificado para firma electrónica avanzada, debe estar vigente y no revocado, al momento de renovar, esta validación la realiza PSC SeguriData al momento en que el cliente accede al portal. En caso de que el certificado este vencido, debe realizar la emisión de un nuevo certificado de manera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



a. 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.

7.3.7 Renovación de certificados después del Vencimiento

La renovación de certificados se presenta únicamente antes de que el certificado venza y hasta 2 semanas antes de su vencimiento, por lo que este caso no aplica como renovación.

Debe procederse a la emisión del certificado de manera presencial.

7.3.8 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 está disponible en el Sitio WEB. En la consulta de estatus de certificados.

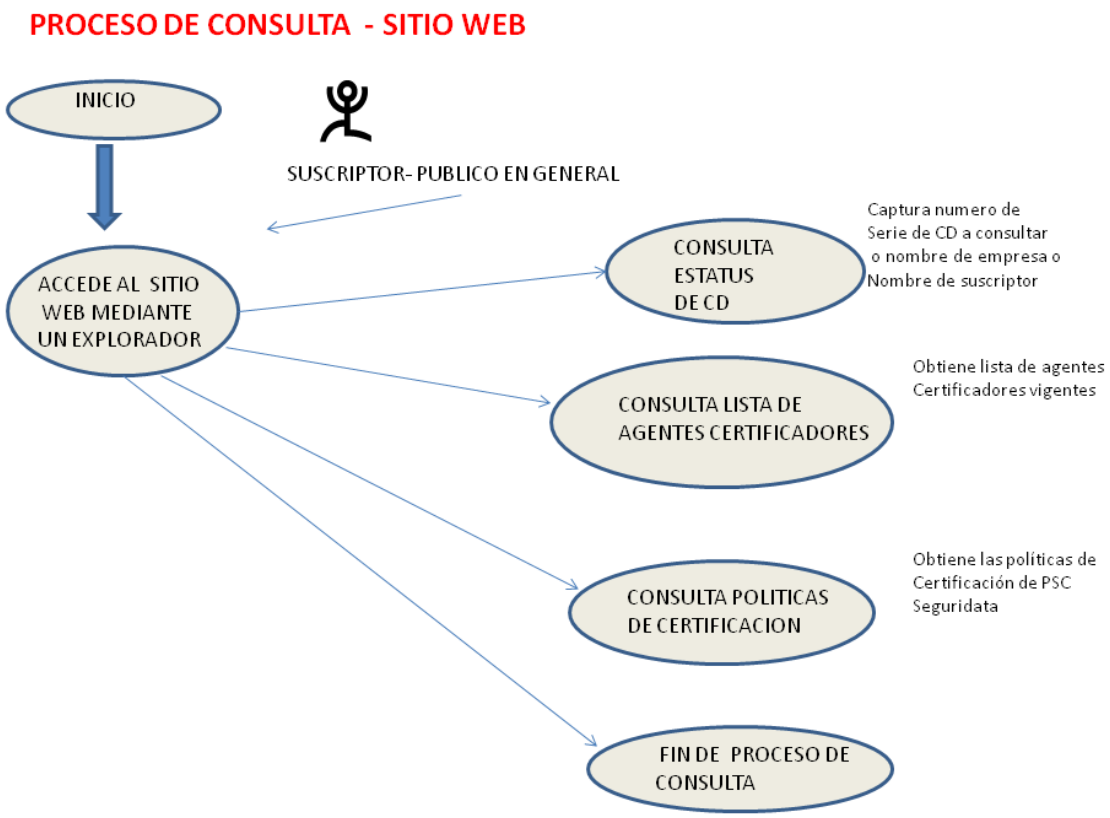
7.3.9 Comprobación de la Disponibilidad de la Revocación/Estado en Línea (OCSP)

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 esté disponible en un tiempo menor al máximo de tiempo establecido 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.



7.3.10 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.

7.3.11 Otras Formas de Publicación de la Revocación Disponible

No se establecen otras formas de Publicación de Revocación disponible.

7.3.12 Circunstancias para Proceder a la Suspensión

El estado de suspensión en los Certificados no está estipulado.

7.4 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.

7.4.1 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 o mediante el servicio de Protocolo de Estado de Certificado en Línea (OCSP), realizando la consulta en el Sitio WEB.

7.4.2 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.

7.4.3 Aspectos Opcionales

Sin estipular.

7.5 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.
- Revocar su Certificado obteniendo uno nuevo.

7.6 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 Gestión, Operación y Controles Físicos

Los controles de seguridad y procedimientos seguidos por la Infraestructura de Clave Pública para las instalaciones, sistemas y el activo de la información serán documentados, puestos en práctica y mantenidos.

8.1 Controles de Seguridad Física

SeguriData Privada S.A. de C.V. gestiona y pone en práctica controles de seguridad apropiados para restringir el acceso al hardware y al software utilizado en relación con la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

SeguriData Privada S.A. de C.V. asegurará que el acceso físico a servicios críticos es controlado y que se tiene el análisis y la reducción de los riesgos físicos de sus activos.

Se ponen en práctica controles para evitar la pérdida, el robo, el daño o el compromiso de activos y la interrupción de la operación de la Infraestructura de Clave Pública. También existen perímetros de seguridad claramente definidos.

Se ponen en marcha controles de seguridad físicos y ambientales para proteger los recursos en los que está alojada la Infraestructura de Clave Pública, aplicando controles de acceso físico, controles de protección y recuperación ante desastres, controles de seguridad contra incendios e inundaciones, controles de fallos en las instalaciones, como por ejemplo, suministros de energía, telecomunicaciones, aire acondicionado, etc.

8.1.1 Ubicación y Construcción

La ubicación de los servicios de la Infraestructura de Clave Pública está en un centro de datos ambientalmente seguro. Dicha ubicación cumple con las normas ISO siguientes:

- NMX-CC-9001-IMNC-2000/ISO 9001:2000, para los procesos de Administración de Cambios, Administración de Incidentes y Administración de las Configuraciones.
- ISO/IEC 20000-1:2005, para la administración de sistemas de Tecnologías de la Información.
- ISO/IEC 27001:2005, para la administración de sistemas de Tecnologías de la Información.

Cualquier equipo relacionado con la Infraestructura de Clave Pública cumple con un conjunto de principios de seguridad mínimos capaz de proporcionar un servicio a prueba de fallos conforme al documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.1.doc, entregado a la Secretaría de Economía con motivo de la acreditación como Prestador de Servicios de Certificación.

8.1.2 Acceso Físico

El personal que entra al área segura donde está la AC, no podrá quedarse sólo por periodos de tiempo significativos sin la supervisión de personal autorizado. En la administración de la AC se protegen datos sensitivos contra accesos no autorizados o modificaciones por red, la AC asegura que el acceso a la información y a las funciones de las aplicaciones del sistema están restringidos de acuerdo a la Política de Seguridad Física del Sitio de Interlomas y Tultitlan, así como de la Política de Seguridad Física de las Oficinas de SeguriData, incluyendo la separación de funciones de administración y operación.

El personal es Autenticado e identificado antes de usar las aplicaciones relacionadas a la administración de la AC, por lo que el personal debe rendir cuentas de sus actos.

8.1.3 Energía Eléctrica y Aire acondicionado

El área segura de operaciones se encuentra conectada a una fuente de energía estándar. Los componentes críticos de la Infraestructura de Clave Pública se encuentran conectados a la fuente de energía ininterrumpida (UPS), para prevenir la interrupción del servicio en caso de interrupciones del suministro eléctrico.

8.1.4 Riesgos por Inundaciones

La ubicación donde se encuentran los servicios de la Infraestructura de Clave Pública proporciona protección contra las inundaciones, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.1.doc.

8.1.5 Prevención de Incendios y Protección

La ubicación donde se encuentran los servicios de la Infraestructura de Clave Pública proporciona protección contra incendios, el detalle de encuentra en el documento PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.1.doc.

8.1.6 Almacenamiento de Medios

Todos los medios de comunicación magnéticos que contienen la información de la Infraestructura de Clave Pública, incluyendo medios de comunicación de respaldos, son almacenados en contenedores, gabinetes o cajas fuertes con capacidad de protección contra incendios.

Se conservan todos los registros de los usuarios y de la AC protegiéndolos contra destrucción y falsificación de acuerdo a la Política de Seguridad de la Información.

8.1.7 Destrucción de Documentos

Los documentos en papel y aquellos medios que contengan elementos sensibles de la Infraestructura de Clave Pública o información comercialmente sensible o confidencial serán eliminados, solo en caso de que la autoridad certificadora de SeguriData Privada SA de CV deje de existir, y será bajo las siguientes condiciones:

- Para información en medios magnéticos:
    - Destrucción completa del mecanismo.
    - El empleo de una utilidad aprobada para limpiar o sobrescribir medios magnéticos.
- Para información en material impreso

  Trituración.

8.1.8 Copias de Seguridad

Se utilizarán elementos de almacenamiento en sitios externos para el resguardo y la retención de las copias de seguridad pertenecientes a la información relacionada con la Infraestructura de Clave Pública, el software de reserva y datos relacionados con elementos críticos especificados en la Política de Certificados.

El almacenamiento en sitio externo se tiene en el Site de Tultitlan:

- Está disponible al personal autorizado 24 horas por día, 365 días del año con el fin de recuperar el software y datos;
- El lugar cuenta con los niveles apropiados de seguridad física.

8.2 Procedimientos de Control

SeguriData Privada S.A. de C.V. asegura que los procedimientos administrativos relacionados con el personal y exigencias procesales, mecanismos de seguridad físicos y tecnológicos, se mantienen conforme a esta Declaración de Prácticas de Certificación, la Política de Certificados y otros documentos operacionales relevantes.

SeguriData Privada S.A. de C.V. asegura que sus sistemas son seguros y se gestionan correctamente, con un riesgo mínimo de fallo. Los perjuicios, incidentes de seguridad y mal funcionamiento serán reducidos al mínimo mediante el uso de sistemas de información de incidentes y procedimientos de respuesta.

SeguriData Privada S.A. de C.V. actuará de una manera oportuna y coordinada para responder rápidamente a los incidentes que puedan surgir.

8.2.1 Roles de Confianza

A fin y efecto de asegurar quien tiene acceso a qué parte del sistema, las responsabilidades se han diferido en varios roles y usuarios para asegurar que las personas actúan dentro de los límites de sus responsabilidades y dentro de la política de seguridad indicada.

Dicha diversificación se ha logrado creando roles separados con sus respectivas cuentas de usuario y certificados digitales, con límites establecidos de acuerdo a las funciones de cada rol.

Los roles implican las responsabilidades siguientes:

- **Oficiales de Seguridad**: responsabilidad total de administrar las prácticas de seguridad.
- **Administradores del Sistema**: Autorizados para instalar, configurar y mantener sistemas.
- **Operadores del Sistema**: Responsables de gestionar el funcionamiento diario de los sistemas. Autorizados para gestionar el sistema de copias de seguridad y recuperación ante fallos;

- **Auditores del Sistema**: Autorizados para ver y mantener archivos y registros de auditoría del sistema.
- **Agente certificador.** Encargado de gestionar la emisión y revocación de certificados digitales
- **Administrador de Base de datos.** Encargado de administrar la base de datos
- **Administrador de redes.** Encargado de la administración de las comunicaciones y redes.

Los roles relevantes del personal serán formalmente designados por el órgano responsable de la seguridad. El personal no tendrá acceso a las funciones relevantes hasta que todas las comprobaciones necesarias sean completadas.

Los procedimientos serán establecidos y puestos en práctica para todas las funciones que afecten a la Infraestructura de Clave Pública.

8.2.2 Número de Personas Requeridas por Tarea

El número de personas requeridas por tarea se da de acuerdo a:

Tarea	Personas requeridas
Emisión y revocación de certificados	Operador de sistemas Administrador de sistemas Agente certificador
Generación de Llaves de la AC	Administrador de sistemas Oficial de seguridad
Administración de la base de datos	Administrador de base de datos
Administrar las comunicaciones	Administrador de redes
Revisar procesos de auditoria y seguridad	Oficial de seguridad

Se llevarán a cabo prácticas para asegurar que una persona que actúa sola no pueda alterar las medidas de seguridad. Para asegurar mejor la integridad de los equipos donde opera la

Infraestructura de Llave Pública, se aplicarán esfuerzos para identificar a un individuo distinto para cada rol de confianza, de acuerdo a la tabla siguiente:

Rol original	Reemplazo temporal de rol
Oficial de seguridad	Profesional Jurídico
Administrador de redes	Oficial de seguridad
Administrador de base de datos	Administrador de redes
Administrador de sistemas	Operador de Sistemas
Operador de sistemas	Administrador de Sistemas

8.2.3 Identificación y Autenticación para cada Función

Las personas que realizan las funciones relevantes están sometidas a una seguridad apropiada. Cada individuo que realiza cualquiera de las funciones relevantes usará un Certificado emitido por la Autoridad Certificadora para identificarse en la Infraestructura de Clave Pública.

8.2.4 Funciones que Requieren Separación de Deberes

Las operaciones que implican la administración de la Autoridad Certificadora son segregadas.

Todas las operaciones que implican el mantenimiento de registros de auditoría son segregadas.

El personal (tanto temporal como permanente) tendrá descripciones de trabajo definidas desde el punto de vista de separación de deberes y privilegios de acceso, determinando la sensibilidad de la posición con base en los deberes y niveles de acceso, los antecedentes, preparación y conocimientos del empleado. Si es apropiado, se diferenciarán funciones generales y específicas. Para ello se recomienda que las descripciones de trabajo incluyan habilidades y requisitos de experiencia.

8.3 Controles de Seguridad Personales

Se llevarán a cabo comprobaciones sobre todas las personas seleccionadas para llevar a cabo un rol de confianza conforme a la seguridad designada que protege el procedimiento, antes de comenzar su actividad.

Con el objetivo de mitigar el riesgo de que un individuo que actúa solo pueda comprometer la integridad de la Infraestructura de Clave Pública o cualquier Certificado, SeguriData Privada S.A. de C.V. realizará las comprobaciones relevantes de los individuos y definirá las tareas que serán responsables a realizar. SeguriData Privada S.A. de C.V. determinará la naturaleza y amplitud de cualquier comprobación, a su propio juicio. Lo anterior describe completamente las obligaciones en cuanto a controles de personal y SeguriData Privada S.A. de C.V. no tendrá ningún otro deber o responsabilidad en lo que a ello concierne. Sin restricción, SeguriData Privada S.A. de C.V. no será responsable de la conducta de un empleado más allá de sus deberes y sobre el que SeguriData Privada S.A. de C.V. carece de control, como los actos de espionaje, el sabotaje, la conducta criminal, o la mala fe.

SeguriData Privada S.A. de C.V. asegurará que las prácticas sobre el personal y la contratación del mismo, realzan y apoyan la validez de las operaciones realizadas dentro de la Infraestructura de Clave Pública.

8.3.1 Requerimientos de Calificación, Experiencia, Calidad y Formación.

SeguriData Privada S.A. de C.V. empleará personal que posea los conocimientos, experiencia y calificación necesaria para poder prestar los servicios que sean apropiados a su puesto de trabajo.

El personal directivo empleado poseerá conocimientos en tecnología de firma electrónica, así como en procedimientos de seguridad para el personal y experiencia en seguridad de la información y prevención de riesgos.

8.3.2 Procedimientos de Comprobación

Los procedimientos de comprobación incluyen, aunque no limitadamente, la comprobación y la confirmación de:

- Empleo anterior
- Referencias profesionales
- Referencias personales
- Formación académica

- Antecedentes penales
- Estatus e historial financiero y crediticio

SeguriData Privada S.A. de C.V. utilizará técnicas de investigación disponibles permitidas por la ley que proporcionen información similar.

8.3.3 Requerimientos de Formación

SeguriData Privada S.A. de C.V. proveerá a su personal de formación interna y externa para mantener los niveles apropiados y requeridos de competencia para realizar su trabajo con el más alto nivel de calidad.

8.3.4 Frecuencia en la Rotación del Trabajo.

SeguriData Privada S.A. de C.V. proporciona y mantiene un programa de rotación de trabajo para mantener los niveles apropiados y requeridos de calidad a través de roles claves.

8.3.5 Sanciones por Conductas Prohibidas

En caso de realización de cualquier tipo de acción no autorizada, se impondrá la sanción correspondiente, marcadas en el plan de continuidad del negocio y recuperación ante desastres, en función de la falta cometida, que va desde 3 llamadas de atención, hasta el despido.

8.3.6 Requisitos de Personal Externo.

SeguriData Privada S.A. de C.V. no apoya el empleo de personal externo para la realización de funciones relevantes.

8.3.7 Documentación Suministrada al Personal

SeguriData Privada S.A. de C.V. proporciona a su personal todos los materiales de formación necesarios para realizar sus funciones de trabajo y sus tareas conforme al programa de rotación de trabajo.

8.4 Auditoría de Procedimientos de Registro

En este subcomponente se describe el registro de eventos y la auditoría de sistemas, implementados con el fin de mantener un entorno seguro.

8.4.1 Tipos de Eventos Registrados

Todos los actos relacionados con la generación de los pares de llaves de la Autoridad Certificadora son registrados. Esto incluye todos los datos de configuración usados en el proceso.

Los tipos de datos registrados incluyen, pero sin carácter limitativo:

- Todos los datos incluidos en cada proceso de emisión de certificado digital serán registrados en la base de datos, para tener una referencia futura en caso de que su uso fuera necesario.
- Las Listas de Revocación de Certificados serán registrados en la base de datos teniendo el último CRL generado.
- Todos los datos de la transacción de revocación de certificados digitales son registrados, en la base de datos
- Toda la documentación presentada para la solicitud de emisión de un certificado digital en conjunto con la propia solicitud y acuerdo firmados por el suscriptor, los cuales se encuentran en un sitio seguro de manera física almacenados en gavetas bajo llave
- Toda la documentación presentada para la revocación de un certificado digital en conjunto con la propia solicitud de revocación firmada por el suscriptor, los cuales se encuentran en un sitio seguro de manera física almacenados en gavetas bajo llave

Todos los registros llevarán la hora debidamente sellada para el caso de emisión y revocación de certificados, y su integridad estará protegida.

La siguiente información está registrada:

- Identidad de la persona que actúa como Agente Certificador que acepta la solicitud de certificado digital;

8.4.2 Frecuencia de Registro

Comprobaciones de los registros son realizadas y contrastadas de manera mensual. Mediante el proceso de generación de reporte de auditoria, mientras que el registro de las transacciones es diario en función de su ocurrencia.

8.4.3 Período de Conservación de los Registros de Auditoria.

Las transacciones son conservadas en la base de datos durante al menos 5 (cinco) años para posibles comprobaciones de auditoría, y al menos 5 (cinco) años para la información de los certificados digitales.

Las transacciones serán almacenadas al menos 5 (cinco) años después de que la Autoridad Certificadora cese sus operaciones.

8.4.4 Protección de los Registros de Auditoria.

Los datos recogidos en la auditoria son revisados con regularidad para evitar cualquier tentativa de violar la integridad de cualquier elemento de la Infraestructura de Llave Pública.

Solo los Oficiales de Seguridad de la Infraestructura de Llave Pública y Auditores pueden ver los registros de auditoría en su totalidad. SeguriData Privada S.A. de C.V. decidirá si algún registro de auditoría en particular tiene que ser visto por un tercero y lo pondrá a su disposición.

8.4.5 Copia de Registros de Auditoría

SeguriData Privada S.A. de C.V. realiza una un respaldo de la base de datos que contiene las transacciones descritas, el cual se efectúa diariamente.

8.4.6 Notificación al Individuo que Genera un Suceso

Cuando se registra un suceso, al emitir el reporte de auditoria y recibir problemas en la integridad de los datos, se procede a restaurar la base de datos con el respaldo correspondiente, de manera que no es necesario notificar del suceso, ya que no afecta a los individuos (suscriptores).

8.4.7 Evaluaciones de Vulnerabilidad

Se llevarán a cabo evaluaciones relativas al sistema de base, amenazas corrientes y riesgos de vulnerabilidad, que abarquen todos los apartados de la Infraestructura de Llave Pública, incluyendo equipos, ubicación física, registros, datos, software, personal, procesos administrativos y comunicaciones. Los procedimientos de evaluación de vulnerabilidad tienen la intención de identificar amenazas y vulnerabilidades de la Infraestructura de Llave Pública, así como determinar un índice de riesgo en base a la existencia de protecciones y prácticas de control. Gracias a ello la dirección podrá llevar a cabo decisiones informadas, determinando como proporcionar un ambiente seguro en el que el riesgo se reduzca a un nivel y a un coste de gestión aceptables para dirección, clientes, y accionistas.

SeguriData Privada S.A. de C.V. realizará una evaluación de riesgo para evaluar los riesgos de seguridad y determinará las exigencias y procedimientos operacionales necesarios.

SeguriData Privada S.A. de C.V. mantendrá un inventario de todos los activos de la información y asignará una clasificación a las exigencias de protección de tales activos, compatible con el análisis de riesgo efectuado.

9 Base de datos Utilizada

Se utiliza Microsoft SQL Server 2005 como base de datos para la autoridad certificadora, dentro de la cual se cuenta con las tablas de agentes, administración, autoridades, certificados, CRL, revocados y tabla de auditoria; que contienen la información relacionada con la emisión de certificados digitales de FEA.

El acceso a las bases de datos se realiza mediante la autenticación de un usuario y password.

Se maneja el log del manejador de base de datos, el cual es revisado durante el día por el administrador de base de datos, para detectar cualquier tipo de anomalía en la operación o accesos no autorizados.

La privacidad de datos está basada en la Ley federal de protección de datos personales en posesión de particulares, considerando:

- Observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad, previstos en dicha Ley.

Con base a:

- La privacidad de los datos personales
- La confidencialidad de la información

- Las medidas de seguridad administrativas, técnicas y físicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado, esto se detallo en la sección de seguridad física y en esta sección de Base de datos, así como en la de Procedimiento para registro de auditoria.

9.1 Respaldo de base de datos

Para llevar a cabo los respaldos se manejara una infraestructura de almacenamiento en cinta de StorageTek a la cual se accede mediante herramientas especializadas, para ejecución y administración de respaldos de VERITAS / LEGATO con la suite de productos de Netbackup / Networker.

El esquema de respaldos a ejecutar sobre la base de datos es:

- El administrador de la base de datos realiza un respaldo de la base de datos a un archivo indicando en que carpeta se guarda para que este archivo cerrado se guarde en cinta.
- Se entregan 2 cintas una es la que se utiliza y reescribe diariamente y la otra se resguarda en la cintoteca del centro de datos de KIO Tultitlan
- site alterno como DRP y se reutilizara cada mes

El esquema de respaldo a ejecutar sobre los archivos cerrados es de un respaldo completo los domingos y respaldos diarios incrementales con un histórico de una semana.

9.1.1 Política de Respaldos

La política contempla la ejecución de un respaldo completo cada 8 días y un respaldo incremental diario entre cada uno de los respaldos completos.

El servicio de respaldo tanto para el Site de Interlomas – principal como el de Tultitlan – alterno, incluye:

- Respaldo completo semanal después de las 20:00 hrs los sábados
- Respaldo diario incremental después de las 20:00hrs
- Respaldo histórico de un mes , último día del mes después de las 20:00 hrs
- Resguardo histórico por mes, en instalaciones de siete de Tultitlan alterno

Se conservara una bitácora de los respaldos efectuados, marcando el servidor, la fecha de respaldo, el tipo de respaldo, la hora de respaldo, el log de la información respaldada

9.2 Procedimiento para registro de Auditoria

El procedimiento se define de acuerdo a los eventos listados en los puntos anteriores, a partir del uso de los productos de software definidos: SeguriServer 6.12, SeguriNotary 4.8, Modulo de auditoria, y su relación con el manejador de base de datos SQL Server 2005.

Para los productos (aplicaciones) SeguriServer y SeguriNotary, se audita a través de los logs (Bitácoras de errores), que son archivos de texto, que en un futuro se tiene contemplado la Firma Electrónica Avanzada de los mismos, usando un certificado para este fin, el cual se emitirá desde la auto certificación, siendo el responsable el administrador de sistemas. Se contempla que el log se firme electrónicamente de manera automática, diariamente por cada transacción registrada, teniendo la fecha y hora.

Y por el modulo de auditoria de los productos, donde al generar una transacción de emisión de certificado o de revocación, se registran de manera segura las transacciones en la base de datos de la autoridad certificadora mediante la generación de pistas de auditoria.

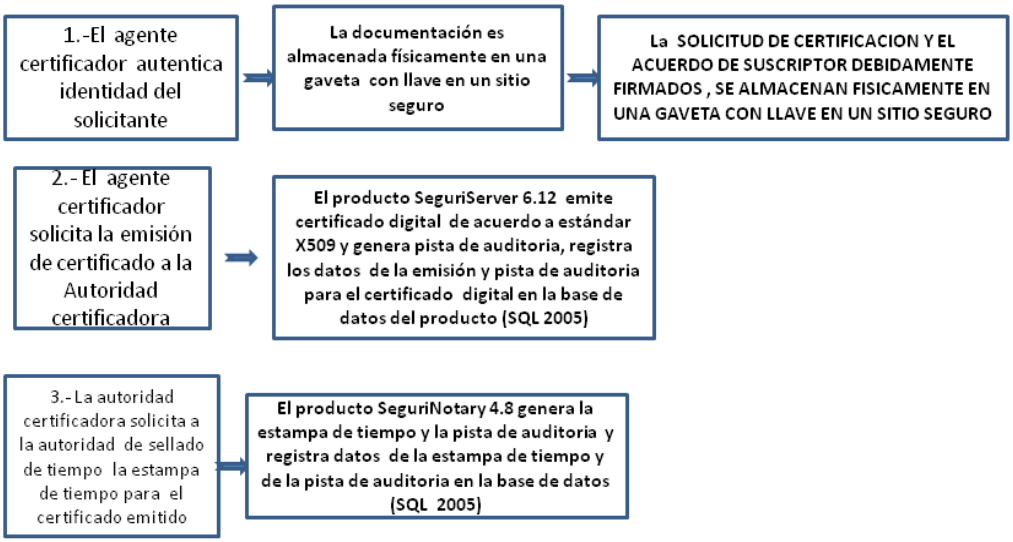
Los datos que se registran en la base de datos son: Numero de secuencia, fecha y hora de la transacción, nombre de la tabla afectada en la base de datos de la autoridad certificadora, y el recibo de auditoria.

Y para el caso de documentación física se establece con relación al resguardo en un sitio seguro en una gaveta asegurada con llave.

A continuación los diagramas de los procedimientos aplicados.

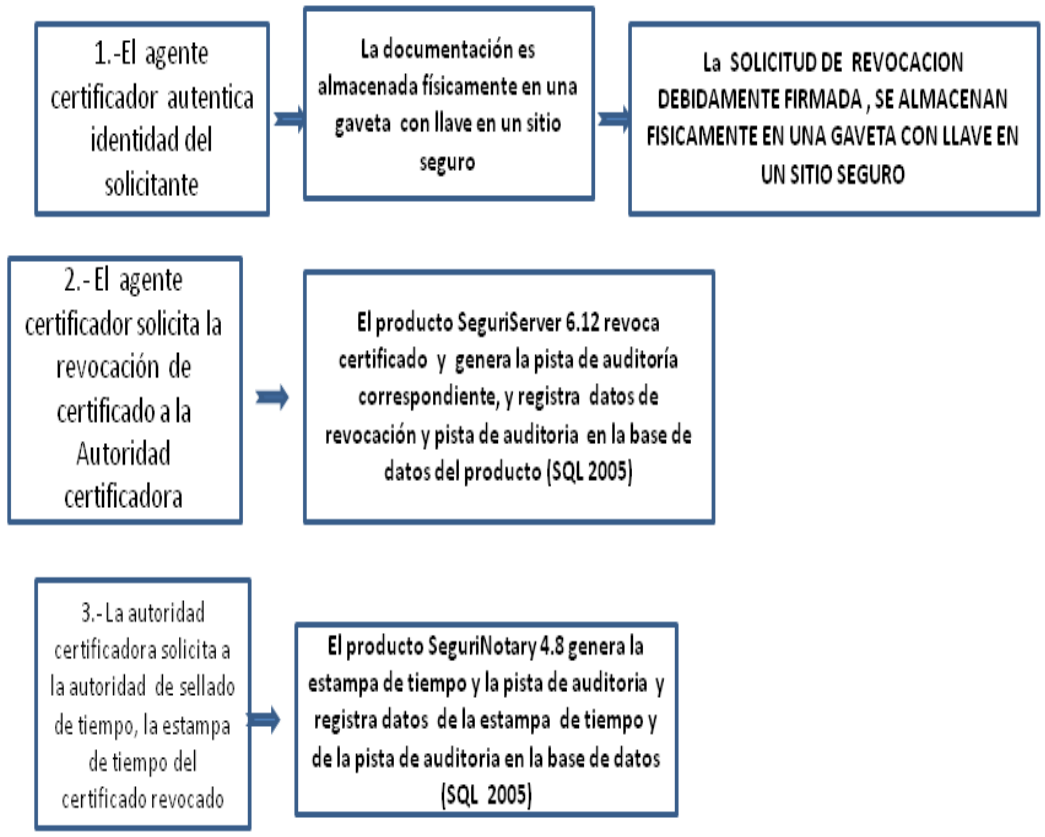
PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS

Registro de datos incluidos en la emisión de Certificados Digitales



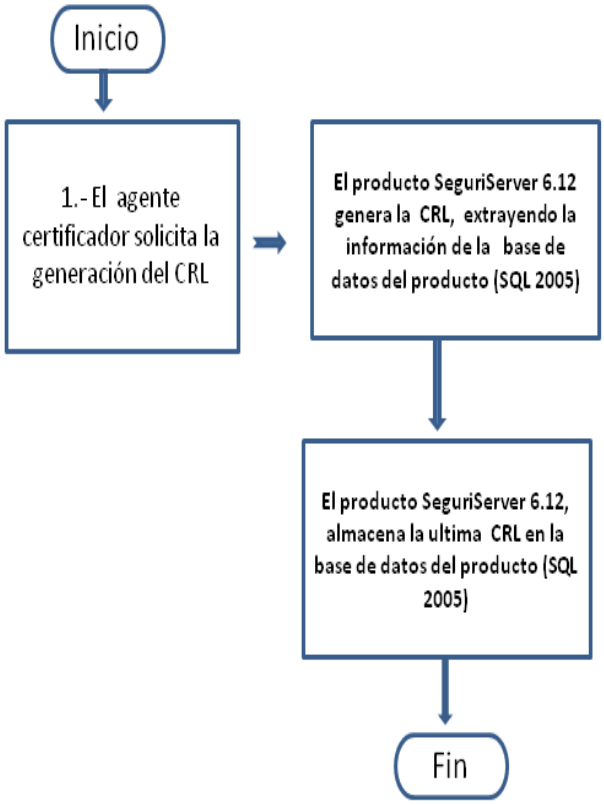
PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS

Registro de datos incluidos en la Revocación de Certificados Digitales



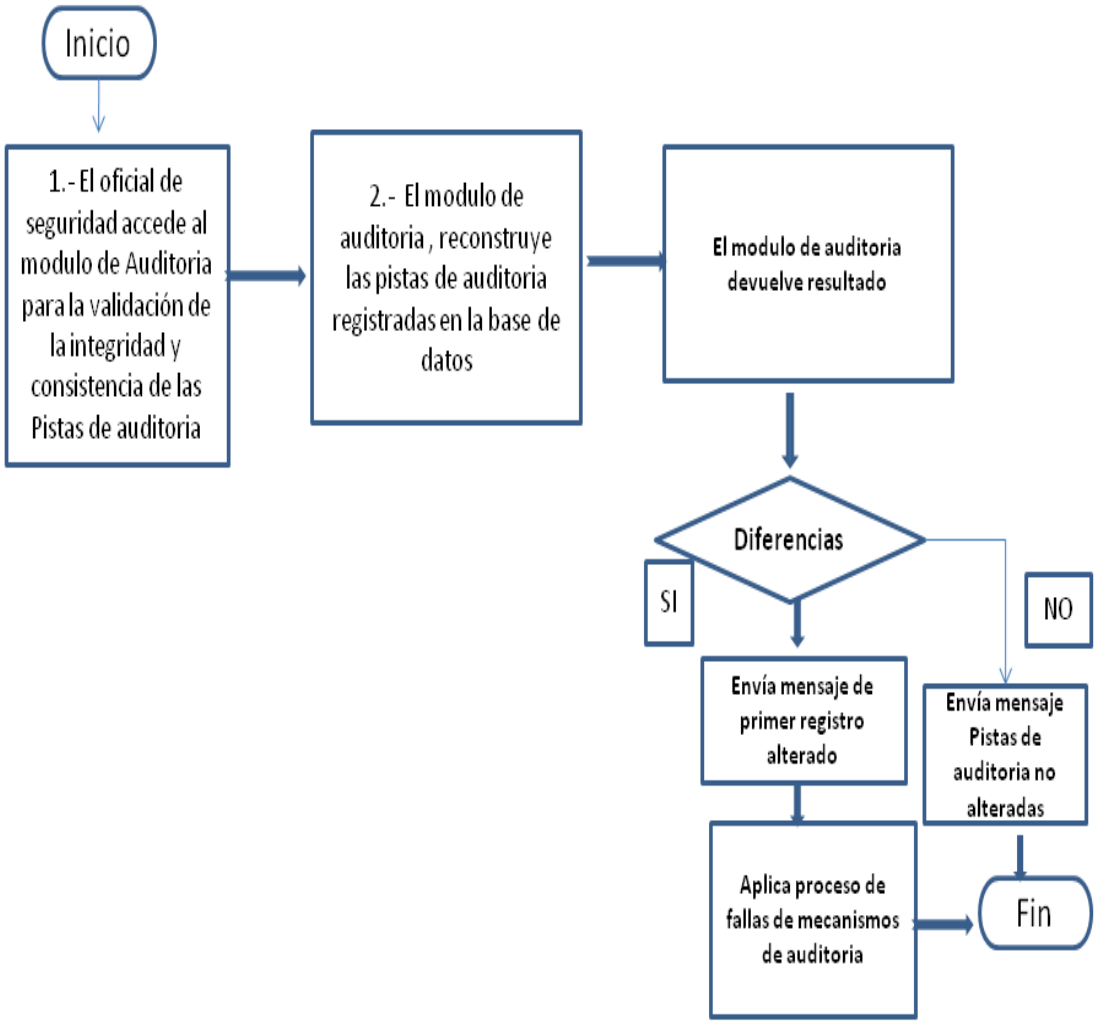
PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS

Registro de datos incluidos en la generación de las CRL's (Listas de certificados revocados)



PROCEDIMIENTO PARA REGISTRO DE AUDITORIA-EVENTOS

Validación de las Pistas de Auditoria



9.3 Archivo de Registros

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de Llave Pública es registrada durante un período apropiado de tiempo, en particular con el objetivo de disponer de pruebas, relativas a los certificados digitales, que se puedan utilizar en procedimientos judiciales.

9.3.1 Tipos de Registros Archivados

SeguriData Privada S.A. de C.V. archiva y hace disponible bajo petición autorizada, la documentación relacionada con este documento. Para cada certificado digital, los registros incluirán la creación, emisión, uso, revocación, expiración. Estos registros incluirán toda la documentación relevante en posesión de SeguriData Privada S.A. de C.V. incluyendo:

- Registros de auditoría. (Información de las pistas de auditoria almacenadas en la base de datos tanto de la emisión del certificado como de la revocación de certificados)
- La solicitud del certificado digital y acuerdos firmados por suscriptores (almacenados físicamente en un sitio seguro en gaveta cerrada con llave)
- Contenido de los certificados digitales emitidos. (almacenada en la base de datos)
- La solicitud de revocación y documentación asociada (almacenados físicamente en un sitio seguro en gaveta cerrada con llave)
- Listas de Revocación de Certificado Digitales (almacenados en la base de datos la ultima CRL generada)
- Nombre del Agente Certificador (en base de datos junto con sus datos)

9.3.2 Período de Retención de Archivos

Los archivos de SeguriData Privada S.A. de C.V. serán conservados y protegidos contra la modificación o destrucción durante un plazo de 5 (cinco) años.

Los registros acerca de certificados digitales serán mantenidos durante el periodo de tiempo necesario para proporcionar las pruebas necesarias para sustentar las firmas electrónicas.

9.3.3 Protección de Archivos

Los archivos serán conservados y protegidos contra la modificación o destrucción. Sólo los Oficiales de Seguridad de la Autoridad Certificadora pueden ver la totalidad de los archivos. El contenido de los archivos no será revelado, salvo que la legislación lo exija. SeguriData Privada S.A. de C.V. puede decidir liberar los registros de transacciones individuales a petición de cualquiera de las entidades vinculadas en la transacción o sus representantes autorizados.

Los archivos serán registrados de modo que no puedan ser suprimidos o destruidos durante el período de conservación necesario.

SeguriData Privada S.A. de C.V. asegurará que toda la información relevante acerca de la Infraestructura de Clave Pública es registrada durante un período apropiado de tiempo, en particular con el objetivo de disponer de pruebas, relativas a los Certificados, que se puedan utilizar en procedimientos judiciales.

9.3.4 Procedimientos de Archivo de Reserva

Se aplicarán procedimientos de reserva adecuados, para que en caso de pérdida o destrucción de archivos primarios haya un juego completo de copias de reserva fácilmente disponible, a través de los respaldos de la base de datos que se hace diariamente y la replicación hacia el Site de Tultitlan como DRP.

9.3.5 Exigencias para el Sellado de Tiempo de los Registros

Todos los acontecimientos registrados dentro del Servicio de la Infraestructura de Clave Pública, como la emisión y revocación de certificados digitales, incluyen la fecha y la hora en el que el acontecimiento ocurrió. Esta fecha y hora se sincronizan con la fecha y hora con que funciona todo el sistema.

Por lo tanto, todas las actividades relacionadas con el Ciclo de Vida del Certificado, quedarán registradas en tiempo. A través del software de SeguriNotary 4.8 que habilita una autoridad de sellado de tiempo.

9.3.6 Sistema de Registro de Archivos (Interno o Externo)

El sistema de registro de archivos de SeguriData Privada S.A. de C.V. es interno.

9.4 Cambio de Clave

El cambio de clave no es automático. Las claves expiran al mismo tiempo que los Certificados asociados y, a excepción de la Autoridad Certificadora que emite un nuevo certificado y claves para sí misma, todos los participantes de la Infraestructura de Clave Pública deben obtener claves nuevas solicitando la emisión de un nuevo Certificado digital al Agente Certificador correspondiente, presentando la documentación requerida.

9.5 Recuperación ante Desastres y la Revelación de Claves

SeguriData Privada S.A. de C.V. dispone de procedimientos para la recuperación después de desastres. El objetivo de estos es restaurar las actividades esenciales con la mayor rapidez posible cuando los sistemas y/o operaciones se han visto considerablemente afectados por incendios, huelgas, terremotos, inundaciones, etc.

SeguriData Privada S.A. de C.V. posee un Plan de Continuidad del negocio y Recuperación ante desastres apropiados, que asegura la continuación inmediata de los servicios en caso de una emergencia inesperada. SeguriData Privada S.A. de C.V. considera su Plan de Continuidad del negocio y Recuperación ante desastres como propio, y susceptible de contener información sensible o confidencial. En consecuencia su contenido no es públicamente disponible.

SeguriData Privada S.A. de C.V. posee un plan frente a la revelación de claves apropiado que detalla sus actividades en caso de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora. Tales proyectos incluyen procedimientos para:

- Revocar todos los Certificados firmados por los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora;
- Notificación inmediata a todos los suscriptores de la Autoridad Certificadora.

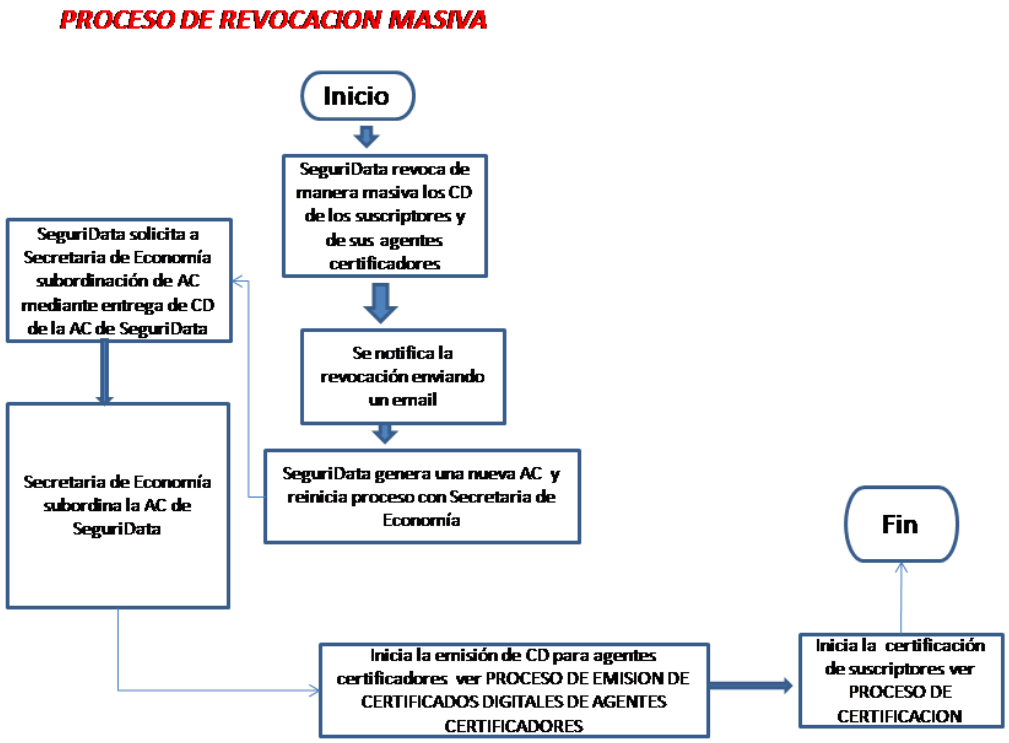
En caso de revelación de claves de la Autoridad Certificadora, SeguriData Privada S.A. de C.V. se compromete al menos a:

- Informar de la revelación de claves a todos los usuarios, terceros de confianza y otras entidades con las que tenga acuerdos u otro tipo de relaciones establecidas;

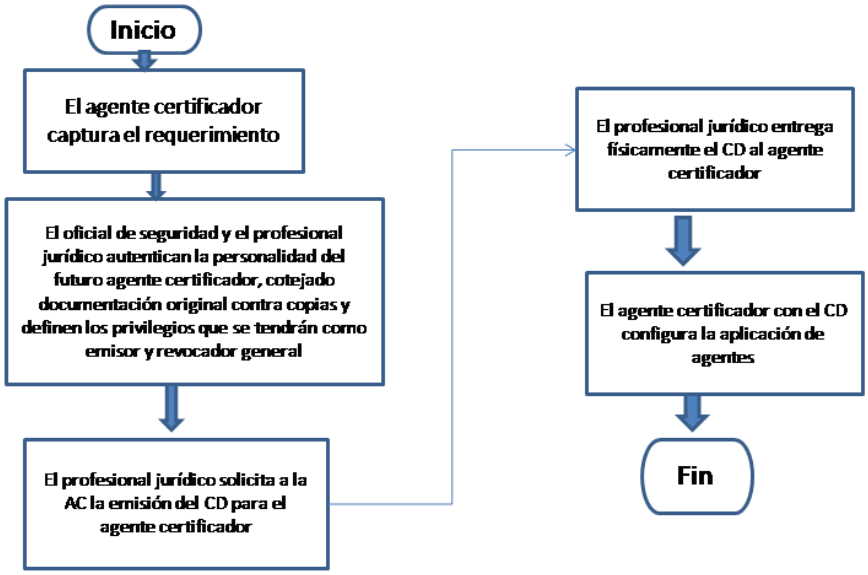
- Indicar que los Certificados y la información de estado de revocación publicada usando estas claves pueden dejar de ser válidos, salvo que cuenten con un sello de tiempo anterior a la revelación de las claves.

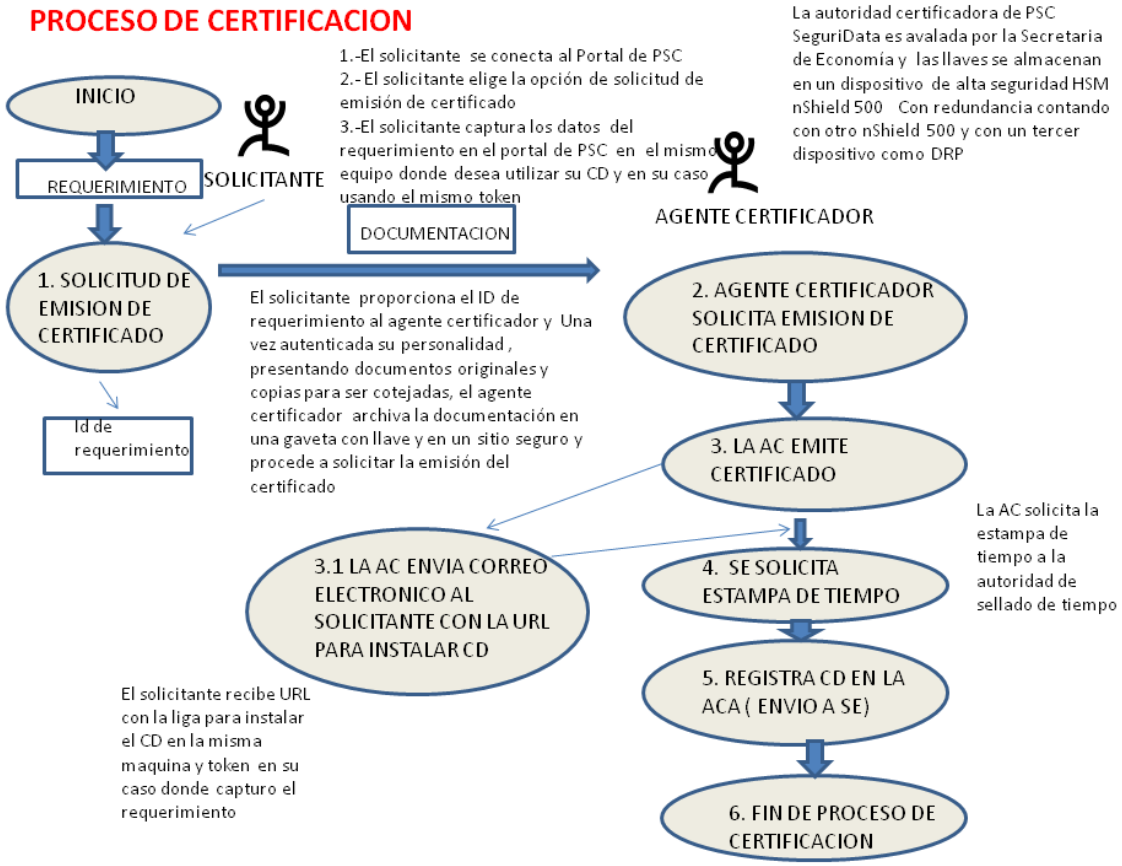
9.5.1 Gestión de Procesos de Incidentes y Revelación de Claves

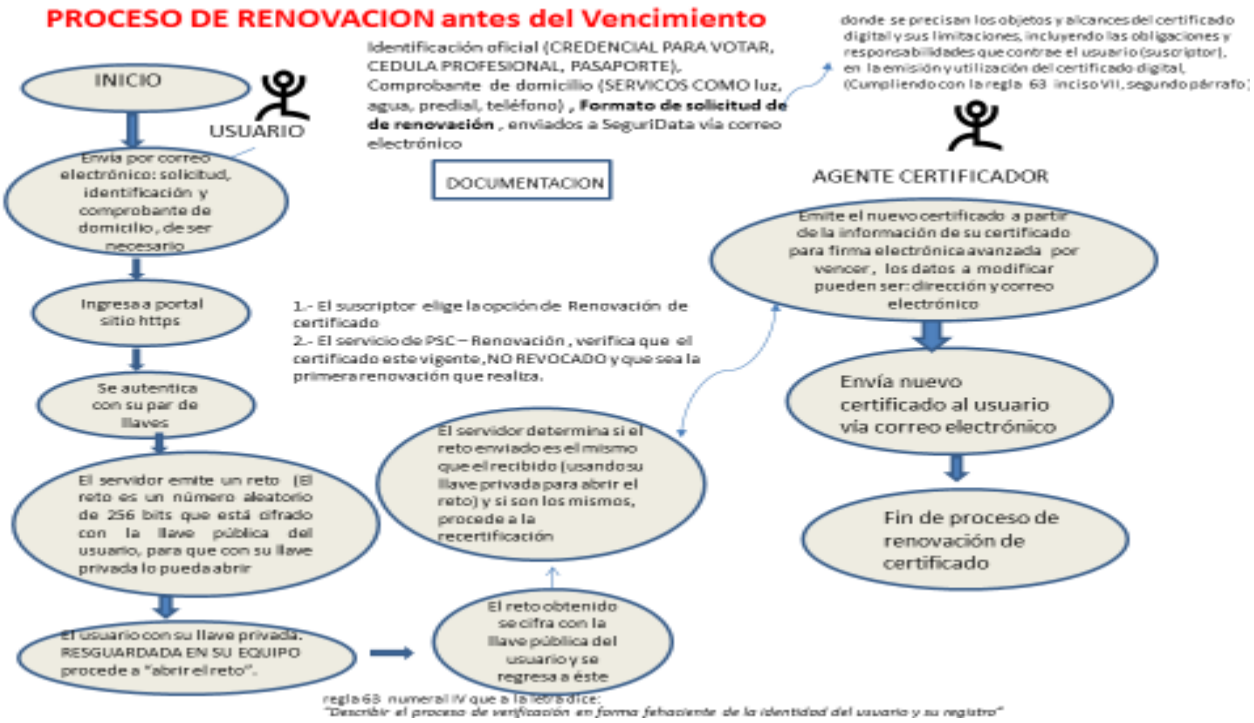
Los procesos asociados son de revocación masiva, emisión de certificados de agentes certificadores y proceso de certificación que a continuación de anexan.



PROCESO DE EMISION DE CERTIFICADOS DIGITALES PARA AGENTES CERTIFICADORES




PROCESO DE CERTIFICACION
La autoridad certificadora de PSC SeguriData es avalada por la Secretaria de Economía y las llaves se almacenan en un dispositivo de alta seguridad HSM nShield 500 Con redundancia contando con otro nShield 500 y con un tercer dispositivo como DRP
1.-El solicitante se conecta al Portal de PSC
2.- El solicitante elige la opción de solicitud de emisión de certificado
3.-El solicitante captura los datos del requerimiento en el portal de PSC en el mismo equipo donde desea utilizar su CD y en su caso usando el mismo token
INICIO
REQUERIMIENTO
SOLICITANTE
AGENTE CERTIFICADOR
DOCUMENTACION
1. SOLICITUD DE EMISION DE CERTIFICADO
Id de requerimiento
El solicitante proporciona el ID de requerimiento al agente certificador y Una vez autenticada su personalidad, presentando documentos originales y copias para ser cotejadas, el agente certificador archiva la documentación en una gaveta con llave y en un sitio seguro y procede a solicitar la emisión del certificado
2. AGENTE CERTIFICADOR SOLICITA EMISION DE CERTIFICADO
3. LA AC EMITE CERTIFICADO
La AC solicita la estampa de tiempo a la autoridad de sellado de tiempo
3.1 LA AC ENVIA CORREO ELECTRONICO AL SOLICITANTE CON LA URL PARA INSTALAR CD
4. SE SOLICITA ESTAMPA DE TIEMPO
5. REGISTRA CD EN LA ACA (ENVIO A SE)
El solicitante recibe URL con la liga para instalar el CD en la misma maquina y token en su caso donde capturo el requerimiento
6. FIN DE PROCESO DE CERTIFICACION



9.5.2 Gestión de Recursos Informáticos, Software, y/o Datos Corrompidos

Estos procedimientos serán detallados en la Política de Certificados.

9.5.3 Procedimientos de Revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora

En caso de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora, los Certificados afectados serán revocados de manera masiva, de acuerdo a los procesos señalados en el Plan de Continuidad del Negocio y Recuperación ante Desastres.

9.5.4 Procedimiento de Continuidad del Negocio tras un Desastre

El Plan de Continuidad del Negocio de SeguriData Privada S.A. de C.V. es estrictamente confidencial y contiene:

- Procedimiento de resolución de incidentes y revelación de claves.
- Gestión de Recursos Informáticos, Software, y/o Datos Corrompidos.
- Procedimiento en caso de revelación de los Datos de Creación de Firma Electrónica.
- Procedimiento de Revocación de Claves Públicas.
- Capacidad de continuidad del negocio y procedimientos después de un desastre.

SeguriData Privada S.A. de C.V. asegurará en caso de un desastre, incluyendo la revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora, que las operaciones serán restauradas cuanto antes.

El Plan de Continuidad del Negocio (o el Plan de Recuperación ante Desastres) tratará como un desastre la revelación o sospecha de revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora.

9.6 Terminación de la Autoridad Certificadora o de las Autoridades de Registro (Agentes Certificadores)

Si fuera necesario liquidar el servicio de la Autoridad Certificadora o el servicio de algún Agente Certificador, el impacto de la liquidación será reducido al mínimo posible.

SeguriData Privada S.A. de C.V. define la política a seguir en caso de terminación total o parcial de su operación en cuanto a la emisión y gestión de los Certificados. La política debe, al menos:

- Asegurar que cualquier interrupción causada por la terminación de la Autoridad Certificadora es reducida al mínimo.
- Asegurar que los archivos de registro de la Autoridad Certificadora son conservados.
- Asegurar que la terminación se notifica puntualmente a los suscriptores, terceros de confianza, y otras partes relevantes en la Infraestructura de Clave Pública.
- Asegurar que se dispone de un proceso para revocar todos los Certificados emitidos por la Autoridad Certificadora en el momento de la terminación.

- Notificar al gobierno competente y a los órganos de certificación relevantes, la terminación de operaciones, de acuerdo con la legislación vigente.

SeguriData Privada S.A. de C.V. asegurará que las interrupciones potenciales a usuarios y terceros de confianza son reducidas al mínimo como consecuencia del cese de servicios de la Autoridad Certificadora, y asegura el mantenimiento continuado de los registros necesarios para proporcionar pruebas de cara a un posible procedimiento judicial.

Antes de que la Autoridad Certificadora cese sus servicios ejecutará los siguientes procedimientos:

- Informará a todos los usuarios, con las que mantenga acuerdos u otro tipo de relaciones vinculantes.
- Terminará toda la autorización de subcontratistas para actuar de parte de SeguriData Privada S.A. de C.V. en el funcionamiento de cualesquiera funciones relacionadas con el proceso de publicación y emisión de certificados.
- Realizará las gestiones necesarias para transferir a un tercero la obligación de mantener la información y archivos de registro de sucesos durante el período respectivo de tiempo pactado con el suscriptor y el tercero de confianza.
- Destruirá o impedirá el uso de sus Datos de Creación de Firma Electrónica.

Declarará en su Práctica de Certificación y Política de Certificados las provisiones hechas para el cese del servicio. Esto incluirá:

- La notificación a las entidades afectadas.
- La transferencia de sus obligaciones a otras partes.
- La gestión del estado de revocación para los Certificados no vencidos que hayan sido emitidos.

9.6.1 Claves de Usuario y Certificados

La revocación de Certificados, será planificada para coincidir con la entrega progresiva de un nuevo Certificado por la Autoridad Certificadora sucesora.

9.6.2 Autoridad Certificadora Sucesora

La Autoridad Certificadora que suceda a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. deberá asumir, en el límite de lo posible, los mismos derechos y obligaciones que tiene la

Autoridad Certificadora de SeguriData Privada S.A. de C.V. La Autoridad Certificadora sucesora deberá emitir nuevas claves y Certificados a todos los proveedores de servicios subordinados y usuarios cuyas claves y Certificados fueron revocados por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. debido a su terminación. Siempre que los solicitantes-suscriptores en cuestión soliciten nuevas claves o certificados y cumplan los requisitos iniciales de registro, identificación y autenticación, incluyendo la firma de un nuevo acuerdo.

La autoridad sucesora es emitida a la mitad de la vigencia de la autoridad certificadora inicial que es de al menos 10 años, por lo tanto se emite a la mitad de su periodo de vida, en este caso a los 5 años, y a partir de ese momento emite certificados digitales para los nuevos suscriptores.

9.6.3 Procedimiento de Destrucción de los Datos de Creación de Firma Electrónica

Todos los suscriptores tienen la obligación de proteger sus Datos de Creación de Firma electrónica avanzada del acceso no autorizado. Los Datos de Creación de Firma electrónica avanzada serán destruidos en un modo que impida su robo, modificación, descubrimiento o uso no autorizado.

En caso de terminación de la Autoridad Certificadora, su personal destruirá los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora.

10Controles de Seguridad Técnica

Los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora están protegidos dentro de un módulo de seguridad criptográfica que cumple con el estándar FIPS (Federal Information Processing Standard) 140-2 nivel 3.

El acceso a todos los módulos dentro del entorno de la Infraestructura de Clave Pública, incluyendo los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora, está restringido por el uso de dispositivos/tarjetas criptográficas y contraseñas. Estas tarjetas criptográficas y contraseñas son distribuidas entre los miembros del equipo de administración de la Infraestructura de Clave Pública. Tal asignación asegura que ningún miembro del equipo posee control total sobre cualquier componente del sistema.

10.1 Generación del Par de Claves e Instalación

La generación del par de claves y su instalación se considera para la Autoridad Certificadora, los Agentes Certificadores y los suscriptores.

10.1.1 Generación del Par de Claves

Todos los Pares de Claves serán generados del modo que a juicio de la Autoridad Certificadora de SeguriData Privada S.A. de C.V., se considere seguro. El suscriptor debe proporcionar toda la información de identificación y autenticación necesaria en el momento de solicitar el Certificado. Una vez que toda la información de registro se haya recogido por el Agente Certificador, el par de claves, para los suscriptores, se generará en un entorno seguro. Los suscriptores pueden generar sus propios Datos de Creación de Firma electrónica avanzada antes de someter una petición de Certificado. Los métodos y requisitos para la generación de claves difieren dependiendo del tipo de Certificado solicitado y deberán consultarse en la Política de Certificados apropiada.

La generación de claves del suscriptor puede ser realizada en hardware o software dependiendo del tipo de Certificado.

10.1.2Entrega del Certificado al Suscriptor

El certificado emitido por la Autoridad certificadora es entregado al suscriptor a través del envió de un correo electrónico con la liga mediante la cual puede instalar el certificado, en la misma máquina donde genero el requerimiento o bien en el mismo token según sea el caso.

10.1.3 Entrega de la Clave Pública de la Autoridad Certificadora a Terceros de Confianza

Las claves Públicas de la Autoridad Certificadora estarán públicamente disponibles en el repositorio, y también en el sitio web corporativo: https://seguridata.psc.com.

10.1.4 Tamaño de las Claves

La longitud de las claves dentro de la Infraestructura de Clave Pública de SeguriData Privada S.A. de C.V. es determinada por los perfiles de los Certificados, y desarrollada más ampliamente en la

Política de Certificados, siendo al menos de 1024 para certificados de suscriptores y al menos de 2048 para autoridad certificadora.

10.2 Protección de los Datos de Creación de Firma electrónica avanzada y Controles a Módulos Criptográficos

Se requiere a todos los participantes en la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. tomar todos los pasos apropiados y adecuados para proteger sus Datos de Creación de Firma electrónica avanzada conforme a las exigencias de esta Declaración de Prácticas de Certificación y la Política de Certificados. Sin perjuicio de lo anterior, todos los participantes en la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. deben:

- Asegurar sus Datos de Creación de Firma electrónica avanzada y tomar todas las precauciones razonables y necesarias para prevenir la pérdida, el daño, el descubrimiento, la modificación, o el empleo inapropiado de sus Datos de Creación de Firma electrónica avanzada (incluyendo la contraseña, los dispositivos u otros datos de activación usados para controlar el acceso a los Datos de Creación de Firma Electrónica);

- Ejercer un control completo y exclusivo sobre el uso de los Datos de Creación de Firma electrónica avanzada y su correspondiente clave pública.

La Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. se asegurará de que:

- Sus claves se generan en circunstancias controladas.

- Sus claves no se usan de manera inapropiada.

- Las claves usadas por la Autoridad Certificadora para generar Certificados, y/o publicar la información del estado de revocación, no serán usadas para ningún otro objetivo.

- Los Datos de Creación de Firma electrónica avanzada serán entregados al solicitante en una manera tal que la privacidad de la clave no se vea comprometida y en la entrega sólo el suscriptor tenga acceso a sus Datos de Creación de Firma Electrónica.

10.2.1 Estándares y Controles del Módulo de Seguridad de Hardware (HSM)

El uso de un dispositivo criptográfico avanzado conocido como un Módulo de Seguridad de Hardware (HSM), permite la generación y el mantenimiento de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora. El Módulo de Seguridad de Hardware usado por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. está diseñado para cumplir el estándar internacional de seguridad FIPS (Federal Information Processing Standard) 140-2 nivel 3, tanto en la generación como en el mantenimiento de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora.

La longitud del algoritmo y la llave seleccionados para el par de claves de la Autoridad Certificadora será RSA de al menos 2048 bits, el cual, es apto para los certificados emitidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. El algoritmo de firma es SHA-1 con RSA.

SeguriData Privada S.A. de C.V. se asegurará de que su llave privada es confidencial y mantiene su integridad. Los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora será mantenida y usada dentro de un dispositivo criptográfico seguro que cumpla las exigencias identificadas en la FIPS PUB 140-2 nivel 3.

10.2.2 Archivo de los Datos de Creación de Firma Electrónica

Los Datos de Creación de Firma electrónica avanzada no serán archivados.

10.2.3 Transferencia de los Datos de Creación de Firma electrónica avanzada hacia o desde un Dispositivo Criptográfico (Token)

En caso de uso de un dispositivo criptográfico (Token), los Datos de Creación de Firma electrónica avanzada deben ser generados en el mismo y permanecer allí tanto en modo cifrado como en descifrado, siendo descifrado sólo en el momento en que se esté utilizando. Los Datos de Creación de Firma electrónica avanzada nunca deben existir en modo de texto simple fuera del módulo criptográfico. En caso de que los Datos de Creación de Firma electrónica avanzada deban ser transportados de un dispositivo criptográfico a otro, deberán ser cifrados durante el transporte.

10.2.4 Clasificación de Dispositivos Criptográficos (Token)

Los dispositivos criptográficos (Token) empleados por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. cumplen con los estándares de la industria. Además, SeguriData Privada S.A. de C.V. garantiza:

- La seguridad del dispositivo criptográfico (Token) durante todo su ciclo de vida
- Que el Token permite que los Datos de Creación de Firma electrónica avanzada se generen en el mismo dispositivo (FIPS 140-2 Nivel 3).

10.3 Otros Aspectos de la Administración del Par de Claves

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. asegurará que la integridad y la autenticidad de las claves públicas de verificación de firmas digitales de la Autoridad Certificadora y cualquier parámetro asociado se conservan durante su distribución a terceros. Dicha clave pública se pondrán a disposición de terceros de manera que se garantice su integridad y se autentique su origen.

10.3.1 Archivado de la Clave Pública

Las claves públicas serán registradas en los Certificados que serán archivados en el repositorio. No se mantendrá ningún archivo separado de claves públicas.

El período de validez de los Certificados dependerá de la clase de Certificado en cuestión según la Política de Certificados.

10.3.2 Período Operativo de los Certificados y del Par de Claves

Los plazos de uso para claves públicas y Datos de Creación de Firma electrónica avanzada coincidirán con los plazos de uso de los Certificados que vinculan la clave pública a un Individuo, Organización, o Dispositivo. Para más información léase el contenido del campo “Válido desde” y “Válido hasta” en los perfiles de los Certificados descritos en la Política de Certificados, los cuales, indican que la vigencia de los Certificados expedidos por la Autoridad Certificadora de SeguriData Privada S.A. de C.V., hacia sus suscriptores es a lo más por un período de dos años.

10.4 Datos de Activación

No aplicable.

10.5 Controles de Seguridad Informática

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. establece un Sistema de Seguridad que cumple los requisitos técnicos de seguridad informática necesarios para las operaciones de la Autoridad Certificadora. El detalle de dichos controles, se encuentra en el documento "PSC-SEGURIDATA-POLITICAS DE SEGURIDAD-SITESANTAFE-INTERLOMAS-VERSION1.0" entregado a la Secretaría de Economía con motivo de la Acreditación a PSC.

Los requisitos técnicos de seguridad informática se alcanzan utilizando una combinación de dispositivos de seguridad y software reforzado, sistema operativo con elementos de seguridad, controles de seguridad físicos y del software en la Infraestructura de Clave Pública y el Agente Certificador, incluyendo la Política de Seguridad y los Procedimientos que incluyen, pero sin carácter restrictivo:

- Acceso controlado a los servicios de la Autoridad Certificadora y roles de la Infraestructura de Clave Pública.
- Identificación y Autenticación del personal que desempeña roles de confianza en la Infraestructura de Clave Pública.
- Archivo histórico y de datos de auditoría de la Autoridad Certificadora.
- Uso de Certificados X.509 V3 para todos los administradores.

La integridad de los sistemas de la Infraestructura de Clave Pública y de la información será protegida contra virus, software malicioso y no autorizado.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. se asegurará de que el acceso a su sistema se limita a individuos correctamente autorizados.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. asegura la administración eficaz del acceso de usuarios (operadores, administradores y cualquier usuario con acceso directo al sistema), para mantener la seguridad del sistema, incluyendo la administración de las cuentas de usuario, la revisión y modificación oportuna o incluso la revocación del acceso.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. asegurará que el acceso a las funciones del sistema de información y de aplicación es restringido y que el sistema proporciona

controles de seguridad informática suficientes para la separación de las funciones relevantes identificadas en la Declaración de Prácticas de Certificación, incluyendo la separación de Oficial de Seguridad y funciones de operadores.

El personal será identificado y autenticado de forma exhaustiva antes de la utilización de usos críticos relacionados con la gestión de Certificados.

10.6 Ciclo de Vida de los Controles de Seguridad

Todo el hardware y software utilizado por la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. debe ser adquirido de manera que se mitigue el riesgo de alteración de cualquier componente particular, como la selección aleatoria de componentes específicos.

El equipo de la Autoridad Certificadora sólo tendrá instaladas aplicaciones o componentes de software que sean parte de la configuración de la Infraestructura de Clave Pública.

Cualquier actualización subsiguiente del equipo de la Autoridad Certificadora debe cumplir los mismos requisitos descritos para el equipo original y ser instalada por personal de confianza y llevado a cabo de una manera definida.

10.6.1 Controles de Desarrollo del Sistema

Un análisis de requisitos de seguridad será realizado durante el diseño y la etapa de especificación de exigencias de cualquier proyecto de desarrollo de sistemas emprendido por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. para asegurar que la seguridad se incorpora a los sistemas de información. Existen procedimientos de control de cambios para liberaciones, modificaciones y situaciones de emergencia en el software para cualquier software operacional.

10.6.2 Controles de Administración de la Seguridad

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. usará sistemas confiables y los productos serán protegidos contra alteraciones.

10.7 Controles de Seguridad de Red

Todo acceso en red al equipo de la Autoridad Certificadora está protegido por cortafuegos de red, Sistemas de Detección de Intrusos (IDS) y enrutadores filtro. Los cortafuegos, IDS y los enrutadores filtro utilizados para el equipo de la Autoridad Certificadora limitan los servicios de este equipo a aquellos estrictamente necesarios para realizar sus funciones. El equipo de la Autoridad Certificadora está protegido contra los ataques de red conocidos.

Todos y cada uno de los puertos de red y servicios no utilizados permanecen apagados. Sólo el software requerido para el funcionamiento de las solicitudes a la Autoridad Certificadora, estará presente en este equipo.

Los Controles (por ejemplo cortafuegos) serán puestos en práctica para proteger los dominios de red internos de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. de los dominios de red externos accesibles por terceros.

SeguriData Privada S.A. de C.V. se asegurará de que los componentes de red locales (por ejemplo enrutadores) se mantienen en un entorno físicamente seguro y sus configuraciones son revisadas de forma periódica para el cumplimiento de las exigencias especificadas por la Infraestructura de Clave Pública.

11Perfiles del Certificado y de la CRL

En este componente se especifica el formato del Certificado y, si se utiliza CRL y/o OCSP, el formato de la CRL y/o OCSP. Esto incluye información de perfiles, versiones y extensiones utilizadas.

11.1 Perfil del Certificado

Todos los Certificados de la Infraestructura de Clave Pública se ajustan a las características de Certificado y Lista de Revocación de Certificado tal y como se especifica en los estándares sobre Certificados RFC 3280 e ITU-T X.509 versión 3.

Para los objetivos de este documento, el Certificado de la Autoridad Certificadora y los Certificados emitidos, así como cualquier otro perfil de Certificado dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. se detalla en la Política de Certificados.

11.1.1 Extensiones del Certificado

Las extensiones de los Certificados son estipuladas en los perfiles de Certificados detallados en la Política de Certificados.

11.1.2 Identificadores de Objeto para algoritmos criptográficos

Para indicar el algoritmo de firma se utilizará el identificador de objeto "Sha1 con RSA" (1.2.840.113549.1.1.5)

Para indicar el algoritmo de la llave pública se utilizará el identificador de objeto "RSA" (1.2.840.113549.1.1.1)

11.1.3 Formas de Nombre

Visto en la sección 5.1 Denominación

11.1.4 Restricciones de Nombre

Visto en la sección 5.1. Denominación

11.1.5 Identificador de Objeto de la Declaración de Prácticas de Certificación

Visto en la sección 2.3 Nombre del documento de identificación

11.1.6 Uso de la extensión 'Restricciones a las Políticas'

No Estipulado.

11.1.7 Sintaxis y Semántica de los calificadores de la Política

Los Certificados emitidos dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. contienen el Identificador de Objeto Digital para esta Declaración de Prácticas de Certificación y la Política de Certificados.

11.1.8 Semántica de tratamiento para la Extensión critica 'Política de Certificación'

No Estipulado.

11.2 Perfil de la CRL

En este subcomponente se abordan temas como los siguientes (en referencia a una definición de perfil independiente, como se define en IETF PKIX RFC 3280):

- Compatibilidad de números de versión en CRLs; y
- CRL´s y el llenado de las extensiones de entrada de la CRL y su criticidad.]

11.2.1 Número(s) de Versión

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. emite Listas de Revocación de Certificados (CRL's) de la versión 2 y 3 X.509 conforme al Certificado PKIX y el perfil de Lista de Revocación de Certificado.

11.2.2 Lista de Revocación de Certificado y Extensiones de Entrada

Todo usuario del software de la Infraestructura Clave Pública debe procesar correctamente todas las extensiones de la Lista de Revocación de Certificado identificadas en el Certificado y el perfil de Lista de Revocación de Certificado.

11.3 Perfil de OCSP

El Protocolo de Estado del Certificado en Línea (OCSP) está habilitado para todos los Certificados dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

11.3.1 Números de Versión

La versión 1 del Protocolo de Estado de Certificado en Línea (OCSP), como se define en el RFC2560, es la que se aplica dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

11.3.2 Extensiones OCSP

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. utiliza las extensiones del estándar OCSP para transferir datos con valor añadido a los terceros de confianza.

12Auditoría de Cumplimiento y Otras Evaluaciones

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. se someterá a una auditoría para determinar el cumplimiento de esta Declaración de Prácticas de Certificación, al menos anualmente. Estas auditorías incluirán la revisión de todos los documentos relevantes mantenidos por SeguriData Privada S.A. de C.V. en cuanto a sus operaciones dentro de la citada Infraestructura de Clave Pública, conforme a este documento, y las políticas y procedimientos aplicables.

12.1 Temas cubiertos por la Auditoría

Los temas cubiertos por una auditoría incluirán, sin carácter limitativo:

- Política de Seguridad y Planificación.
- Seguridad Física.
- Evaluación de Tecnología.
- Servicios de Administración.
- Acuerdos

12.2 Acciones a Tomar en caso de recomendaciones o hallazgos

Las acciones tomadas como consecuencia de la existencia de hallazgos serán determinadas en función de la naturaleza y grado del hallazgo identificado. Cualquier decisión tomada por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. será acorde a los datos proporcionados por los auditores. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. determinará a su propio juicio un procedimiento y plazos apropiados para rectificar los hallazgos.

13Otros Asuntos Comerciales y Asuntos Legales

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. es una entidad legalmente constituida de acuerdo con la legislación aplicable.

Las partes de la Infraestructura de Clave Pública implicadas en la generación de Certificados y la gestión de revocación serán independientes de otras organizaciones en sus decisiones que se relacionen con el establecimiento, aprovisionamiento, mantenimiento y suspensión de servicios; en particular su equipo directivo, el personal competente y el personal encargado de las funciones relevantes deben estar libres de presiones comerciales, financieras y otras que pudieran influir desfavorablemente en la confianza en los servicios que proporcionan.

13.1 Tarifas

La emisión de Certificados por parte de la Autoridad Certificadora y de los Agentes Certificadores dentro de la Infraestructura de Clave Pública de SeguriData Privada S.A. de C.V. harán disponible todas las tarifas aplicables por la solicitud. Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

13.1.1 Tarifas de Emisión de Certificados

Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

13.1.2 Tarifas de Revocación o Acceso a la Información de Estado del Certificado

Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

13.1.3 Tarifas por otros Servicios

Para consultar las tarifas favor de comunicarse a SeguriData Privada S.A. de C.V.

13.2 Responsabilidad Financiera

La Autoridad Certificadora de SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación dispone de recursos financieros para cubrir los daños que pudiesen surgir debido a su operación, de acuerdo a las disposiciones contenidas en el Reglamento del Código de Comercio en Materia de Prestadores de Servicios de Certificación y las Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. tiene la estabilidad financiera y recursos requeridos para funcionar conforme al documento "COMPROBACION DE CAPITAL PARA INVERSION EN PROYECTO PSC" entregado a la Secretaría de Economía para la acreditación como Prestador de Servicios de Certificación.

13.2.1 Otros Activos

La Autoridad Certificadora y los Agentes Certificadores mantendrán los activos y recursos financieros necesarios para realizar sus deberes dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. y serán razonablemente capaces de afrontar sus responsabilidades frente a suscriptores y terceros de confianza.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. posee los sistemas de calidad adecuados para conseguir la seguridad en la información acorde con los servicios de certificación que proporciona.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. emplea un número suficiente de personal que tiene, en relación con el tipo, gama y volumen de trabajo, la formación, conocimientos técnicos y experiencia necesarios para proporcionar servicios de certificación.

13.2.2 Cobertura de Seguros o Garantías para Entidades Finales

No estipulado.

13.2.3 Registros Financieros

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. es responsable de mantener sus libros financieros y registros en una manera comercialmente razonable.

13.3 Confidencialidad de la Información Comercial

Este subcomponente contiene disposiciones relativas al tratamiento de la información comercial confidencial que los participantes pueden comunicarse entre sí, tales como los planes de negocio, información de ventas, secretos comerciales, e información recibida de un tercero en virtud de un acuerdo de confidencialidad.

13.3.1 Alcance de la Información Confidencial

Cualquier información personal o corporativa mantenida por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. y relativa a un suscriptor y la emisión de Certificados es considerada confidencial y no será divulgada sin el consentimiento previo del usuario afectado, a no ser que sea legalmente exigible, de acuerdo con los requisitos de esta Declaración de Prácticas de Certificación.

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no tiene acceso a los Datos de Creación de Firma electrónica avanzada de los Certificados de cualquiera de los usuarios o entidades a los que certifica. La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no está en absoluto obligada a disponer de copia de los Datos de Creación de Firma Electrónica, con sistema alguno de copia de seguridad, almacenamiento o resguardo.

Los registros que contengan información relevante serán protegidos de la pérdida, destrucción o falsificación. Algunos registros pueden tener que ser conservados para cumplir con las exigencias legales, o para asegurar actividades de negocio esenciales.

13.3.2 Información No Confidencial

La Información incluida en los Certificados, o almacenada en el repositorio no es considerada confidencial, a no ser que la legislación o acuerdos contractuales determinen lo contrario.

13.3.3 Responsabilidad de Proteger la Información Confidencial

Se tomarán medidas técnicas y de organización contra el uso no autorizado o ilegal de datos personales y contra la pérdida accidental, destrucción o daño a los datos personales.

13.4 Política de Privacidad de Datos Personales

Al ofrecer SeguriData Privada S.A. de C.V. los servicios como Autoridad Certificadora, como Prestador de Servicios de Certificación, se tuvo que apegar a varios lineamientos y revisiones metodológicas por la Secretaría de Economía, donde se validara la seguridad de las instalaciones y procesos.

La información que obtiene de los usuarios la Autoridad Certificadora no será utilizada para ninguna publicación de información que divulgue la información de los usuarios. Por lo que no se venderá o traspasará ningún dato que haya proporcionado algún usuario en su solicitud de certificación para fines de promoción.

La Autoridad Certificadora dispone de los procedimientos en este documento, que aplica en la prestación de sus servicios, en el que, en cumplimiento de los requisitos establecidos por la política de certificados, y de acuerdo con el Código de Comercio y a las Reglas Generales para los Prestadores de Servicios de Certificación del 14 de mayo de 2018, se detallan los requisitos y obligaciones en relación con la obtención y gestión de los datos personales que obtenga.

13.4.1 Información Considerada Privada

Toda información sobre los suscriptores no disponibles públicamente por el contenido de los Certificados emitidos, los directorios de Certificados y los repositorios en línea se considerará privada.

13.4.2 Archivos de Registro

Todos los registros son considerados información confidencial y tratados como privados.

13.4.3 Revocación de Certificado

La razón por la que un Certificado ha sido revocado, se considera información confidencial, con la excepción exclusiva de la revocación por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. del Certificado debido a:

- La revelación de los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora, en cuyo caso se puede difundir que los Datos de Creación de Firma electrónica avanzada han sido comprometidos.
- La terminación de servicio de la Autoridad Certificadora, hecho que se puede difundir antes de la terminación.

13.4.4 Información No Considerada Privada

Entre la información que no se considera privada dentro de la Infraestructura de Clave Pública se tienen los siguientes elementos:

- Contenido del Certificado: El contenido de los Certificados publicados por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. es información pública, no confidencial.
- Lista de Revocación de Certificado (CRL) no se califican como información confidencial.
- Declaración de Prácticas de Certificación: Esta Declaración de Prácticas de Certificación de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. es un documento público y no se considera información confidencial.
- Política de Certificados.

13.4.5 Consentimiento para el Uso de Información Privada

Cuando se produce la aceptación de un Certificado, todos los suscriptores acuerdan que sus datos sean tratados y registrados por parte de la Autoridad Certificadora de SeguriData Privada S.A. de C.V., y usados tal y como se especifica en el proceso de registro. Los Usuarios podrán impedir el uso de sus datos personales para determinados objetivos. En cualquier caso deben permitir que algunos de sus datos personales aparezcan en directorios públicamente accesibles y que sean comunicados a terceros.

13.4.6 Revelación de Datos de Conformidad con un Proceso Judicial o Administrativo

La información que los usuarios aporten a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. será totalmente protegida de su revelación salvo consentimiento del usuario, orden judicial u otra autorización legal.

Sólo en el caso de que un Tribunal exija esta información a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. o cualquiera de sus Agentes Certificadores, tal información será revelada si lo exige un procedimiento civil o administrativo.

13.4.7 Otras Circunstancias de Revelación de Información

La Autoridad Certificadora y los Agentes Certificadores no tienen obligación alguna de revelar información al margen de una orden judicial legítima y acorde a la ley, que cumpla con las exigencias de esta Declaración de Prácticas de Certificación.

13.5 Derechos de Propiedad Intelectual

Los Datos de Creación de Firma electrónica avanzada y claves públicas son propiedad del usuario legítimo de dichas claves. Los Certificados emitidos y todos los derechos de propiedad intelectual que incluyen todos los derechos de autor en todos los Certificados y todos los documentos pertenecen a la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

Esta Declaración de Prácticas de Certificación y las Marcas y signos distintivos son propiedad de la Autoridad Certificadora de SeguriData Privada S.A. de C.V.

13.5.1 Licencias

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. está en posesión de licencias de uso del hardware y el software utilizado en la Infraestructura de Clave Pública de SeguriData Privada S.A. de C.V., tal y como se especifica en esta Declaración de Prácticas de Certificación.

13.6 Representaciones y Garantías

Este subcomponente puede incluir representaciones y garantías de diversas entidades que se realizan en conformidad con la Política de Certificados o la Declaración de Prácticas de Certificación.

13.6.1 Garantías de la Autoridad Certificadora

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. por la presente garantiza

1. Que ha llevado a cabo los procedimientos necesarios para verificar que la información contenida en cualquier Certificado es exacta y veraz en el momento de su emisión.

2. Que los Certificados serán revocados si la Autoridad Certificadora de SeguriData Privada S.A. de C.V. cree o se le ha notificado que el contenido del Certificado es inexacto, o que la clave asociada con un Certificado ha sido comprometida de cualquier modo.

La naturaleza de los pasos que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. toma para verificar la información contenida en un Certificado varía según el tipo de Certificado, la naturaleza y la identidad del usuario del Certificado, y los usos para los que el Certificado será estipulado.

La Autoridad Certificadora y todos los Agentes Certificadores deben incorporar, mediante referencias o de otro modo, en los contratos con los suscriptores o en los términos y condiciones aplicables, las garantías, si las hubiere, proporcionadas por la Autoridad Certificadora de SeguriData Privada S.A. de C.V. a los Usuarios y Terceros de Confianza en conexión con esta Declaración de Prácticas de Certificación.

13.6.2 Garantías de Agente Certificador

Por la presente, los Agentes Certificadores autorizados que funcionan dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. garantizan que:

1. Toman las medidas razonables para verificar que la información contenida en cualquier Certificado es exacta en el momento de su emisión.

2. Los Certificados serán revocados si la Autoridad Certificadora de SeguriData Privada S.A. de C.V. cree o se le ha notificado que el contenido del Certificado es inexacto, o que la clave asociada con un Certificado ha sido comprometida de cualquier modo.

13.6.3 Garantías del Suscriptor

Los suscriptores representan y garantizan:

1. Que los Datos de Creación de Firma electrónica avanzada sean protegidos y que nunca otra persona haya tenido acceso.

2. Todas las representaciones hechas por el suscriptor en el uso de Certificado son verdaderas.

3. Toda la información que contiene el Certificado es verdadera y exacta.

4. El Certificado va a ser usado para su objetivo intencionado, aprobado y legal compatible con esta Declaración de Prácticas de Certificación.

13.6.4 Garantías de los Terceros de Confianza.

Los Terceros de Confianza representan y garantizan:

1. Recabar la suficiente información sobre un Certificado y su usuario correspondiente, incluyendo la verificación de estado en línea por el servicio de validación para llevar a cabo una decisión informada en cuanto al grado de seguridad y confianza en el Certificado.

2. Que la parte que confía sea únicamente responsable de tomar la decisión de confiar en un Certificado.

3. Que el tercero de confianza asumirá las consecuencias legales de la falta de cumplimiento de las obligaciones del tercero de confianza según los términos de esta Declaración de Prácticas de Certificación y el acuerdo que haya suscrito.

13.6.5 Garantías de Otros Participantes

Los participantes dentro de la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. se obligan a aceptar y realizar todas y cada una de las obligaciones contenidas en esta Declaración de Prácticas de Certificación.

13.7 Exclusiones en Garantías

No aplica.

13.8 Limitaciones de Responsabilidad

Este subcomponente puede incluir limitaciones de responsabilidad en la Política de Certificados o en la Declaración de Prácticas de Certificación o limitaciones que aparecen o deben aparecer en un acuerdo asociado con la Política de Certificados o en la Declaración de Prácticas de Certificación, tales como un acuerdo de suscriptor o un acuerdo con terceros.

13.8.1 Responsabilidad de la Autoridad Certificadora

La Autoridad Certificadora se responsabilizará frente a los suscriptores o terceros de confianza de cualquier daño que derive del incumplimiento de esta Declaración de Prácticas de Certificación o para cualquier otra responsabilidad en la que pudiera incurrir en el contrato, incluyendo la responsabilidad de la negligencia por cualquier acontecimiento o acontecimientos relacionados.

13.8.2 Exclusiones de Responsabilidad

La Autoridad Certificadora de SeguriData Privada S.A. de C.V. no asumirá absolutamente ninguna responsabilidad de cualquier daño causado por alguna de las siguientes causas:

- Si el Certificado 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 Certificado y/o su llave privada.

- 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 la Política de Certificados.

- Si el Certificado bajo el control del reclamante ha sido usado más allá de los límites de certificación digitales sobre los límites de uso o sobre el valor de transacciones.

- Si el reclamante no ha reclamado la revocación en caso de duda sobre la confidencialidad de los datos de creación de firma.

- Si el reclamante no ha informado a la Autoridad Certificadora de SeguriData Privada S.A. de C.V. sobre los cambios en los hechos proporcionados por el suscriptor para generar el Certificado;

- Si se ha desarrollado hardware, software, o algoritmos matemáticos, que convierta 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.

- Si se ha producido una interrupción prolongada o generalizada del suministra eléctrico, siempre que la Autoridad Certificadora de SeguriData Privada S.A. de C.V. use métodos comercialmente razonables de protección contra tales perturbaciones.

- El fallo de uno o más sistemas informáticos, de infraestructura de las comunicaciones, de tratamiento o almacenamiento 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: una catástrofe (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 (incluyendo, sin restricción, las limitaciones a la exportación); 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 sujeto; y cualquier acontecimiento o circunstancia fuera del control de SeguriData Privada S.A. de C.V.

13.8.3 Aceptación de la Limitación de Responsabilidad

Los Certificados incluyen una declaración breve que detalla las limitaciones de responsabilidad y las exclusiones de la garantía, con una referencia al texto completo de tales advertencias, limitaciones y negaciones en la Política de Certificados. Con la aceptación de un Certificado, la parte reconoce y está de acuerdo con todas las limitaciones y exclusiones.

13.9 Indemnizaciones

No Aplica

13.10 Entrada en Vigor y Terminación

Este subcomponente puede incluir el período de tiempo en el que la Declaración de Prácticas de Certificación permanece en vigor y las circunstancias bajo las cuales se puede terminar el documento, porciones del documento, o su aplicabilidad a un participante concreto.

13.10.1 Entrada en Vigor

Esta Declaración de Prácticas de Certificación entra en vigor a partir de su Publicación en la página web seguridata.psc.com/.

13.10.2 Terminación

Esta Declaración de Prácticas de Certificación permanecerá en vigor hasta que sea modificada o substituida por una versión nueva.

13.11 Avisos Individuales y Comunicación con los participantes

Los Avisos Individuales y comunicaciones con los participantes se llevarán a cabo en la forma que el participante determinó en la solicitud de Certificado.

13.12 Modificaciones

No Aplica

13.13 Procedimientos de Resolución de Controversias

Cualquier controversia o reclamación entre dos o más participantes en la Infraestructura de Clave Pública de la Autoridad Certificadora de SeguriData Privada S.A. de C.V. surgida con arreglo a esta Declaración de Prácticas de Certificación se someterá a un tribunal de arbitraje.

13.14 Ley de Administración

No Aplica

13.15 Cumplimiento con la Ley Aplicable

No Aplica

13.16 Disposiciones Varias

No Aplica

13.17 Otras Disposiciones

No Aplica

13.17.1 Cese de la Autoridad Certificadora

Las causas por las que puede ocurrir el cese de operaciones de la Autoridad Certificadora de SeguriData Privada S.A. de C.V., como Prestador de Servicios de Certificación, es que se hayan comprometido los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora, o por toma de decisión de cese de actividades por parte de SeguriData Privada S.A. de C.V.

13.17.2 Suspensión de la Autoridad Certificadora

La suspensión se puede llevar a cabo de manera temporal o definitiva.

En caso de suspensión temporal, la Autoridad Certificadora de SeguriData Privada S.A. de C.V., anunciará desde el primer momento en que tenga conocimiento de la suspensión temporal como Prestador de Servicios de Certificación, y ejecutará lo siguientes:

Informar mediante el de la Suspensión temporal.

Tratar de restablecer el servicio a la brevedad.

Anunciar mediante el Sitio WEB, cuando se tenga fecha de restablecimiento del servicio.

En caso de suspensión definitiva, la Autoridad Certificadora de SeguriData Privada S.A. de C.V., anunciará desde el primer momento en que tenga conocimiento de la suspensión definitiva como Prestador de Servicios de Certificación, y ejecutará lo siguientes:

- Informar mediante el Sitio WEB de la Suspensión definitiva.
- Revocar los certificados vigentes.
- Gestionar con la Secretaría de Economía la transferencia de los Certificados revocados de sus suscriptores, así como cualquier información importante que pueda requerirse, para que la Secretaría de Economía se haga cargo de los certificados durante la vigencia que se haya cortado, derivado de la suspensión definitiva.
- Destruir los Datos de Creación de Firma electrónica avanzada de la Autoridad Certificadora.

13.18Obligaciones, Políticas y Procedimientos aplicables a Organizaciones Externas

Para el caso de Organizaciones Externas que apoyan el proceso de certificación, se tiene el caso de Xertix-Diveo-Redit,KIO las obligaciones se presentan en el documento addendum al contrato con Diveo, el cual hace referencia a los sitios de Interlomas como principal y Tultitlan como alterno contemplando infraestructura, enlaces y Firewall.

Los procedimientos para el caso de organizaciones externas se mencionan en el documento de Plan de Continuidad del Negocio y Recuperación ante Desastres, donde se menciona también como organización externa al proveedor DELL que maneja los equipos físicos que forman la infraestructura de la Autoridad Certificadora.

14. Protección de Datos y resguardo de expedientes

PSC SeguriData como Autoridad certificadora tiene el compromiso de resguardar y cumplir las disposiciones contenidas en el Código de Comercio, Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, o todas aquellas Leyes o Normas aplicables o relacionadas sobre la seguridad de 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, renovación o revocación de un certificado digital.

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.