



## POLÍTICAS

---

Para el servicio de Constancias de conservación de mensajes de datos emitidas de conformidad con la NOM-151-SCFI-2016

**Legalex GS, S.A. De C.V.**

Morelia, Michoacán; 2021

**OID: 2.16.484.101.10.316.100.6.1.2.1.1**

**VERSIÓN PÚBLICA**



Esto es una versión pública y no contiene todo el material completo de las Políticas de Constancias de Conservación de Mensajes de Datos de Legalex GS, ya que expone la seguridad de la empresa.

Para más información, contacte al Director Ejecutivo de Legalex GS S.A. de C.V.

**POLÍTICAS DE CONSTANCIAS DE CONSERVACION DE MENSAJES DE DATOS**  
LEGALEX GS, S.A. DE C.V.

**OID: 2.16.484.101.10.316.100.6.1.2.1.1**

LEGALEX GS S.A. DE C.V.

LGS160502EA8

Derechos reservados.

LEGALEX GS S.A. DE C.V.

Copyright © 2016-2021

Periférico paseo de la Republica 2650,

Número interior B, piso 2.

Prados del Campestre, C.P. 58297.

Morelia, Michoacán, México.

Teléfono: (01 443) 690 68 51 ó 52

E-mail: [contacto@legalexgs.com](mailto:contacto@legalexgs.com)

## Contenido

Identificación del documento.....	4
Responsables.....	4
Autorización.....	5
Introducción.....	6
Alcance.....	6
Enfoque.....	6
Administración de cambios de las Políticas de Constancias de Conservación de Mensajes de Datos.....	6
Actores y entidades participantes en la infraestructura de la Emisión de Constancias de Conservación de Mensajes de Datos.....	7
Conceptos generales.....	7
Servicio de Emisión de Constancias de Conservación de Mensajes de Datos.....	7
Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD).....	8
Suscriptores o Cliente.....	9
Política de Constancias de Conservación de Mensajes de Datos.....	9
Identificación.....	9
Comunidad de usuarios y aplicabilidad.....	10
Conformidad.....	10
Ciclo de vida de las llaves.....	11
Constancias de Conservación de Mensajes de Datos.....	11
Estructura de las Constancias de Conservación de Mensajes de Datos.....	11
Algoritmo de encriptación de datos.....	12
Obligaciones y responsabilidades.....	12
Obligaciones.....	12
Obligaciones del PSC.....	12
Obligaciones de los Suscriptores o Clientes.....	13
Obligaciones de la parte que confía.....	14
Responsabilidades del PSC.....	14
Responsabilidades de los suscriptores o clientes.....	15
Descarto de responsabilidades.....	15
Limitaciones del servicio.....	15
Responsabilidades Económicas.....	16
Términos y condiciones.....	16
Anexos.....	17

Apéndice A.....	17
Acrónimos.....	17
Glosario.....	18
Apéndice B.....	19
Bibliografía .....	19

## Tabla de cuadros y esquemas

TABLA 1 IDENTIFICACIÓN DEL DOCUMENTO .....	4
TABLA 2 RESPONSABLES DE REVISIÓN.....	4
TABLA 3AUTORIZACIÓN .....	5
TABLA 5ACRÓNIMOS .....	18
TABLA 6DEFINICIONES .....	18

## Identificación del documento

En esta sección se identifican los datos principales del documento:

<b>Nombre</b>	<b>Políticas de Constancias de Conservación de Mensajes de Datos</b>
<b>Versión</b>	1.2
<b>Autor</b>	Legalex GS.
<b>Estado</b>	En elaboración.
<b>Fecha de emisión</b>	30 de junio de 2019.
<b>Fecha de actualización</b>	03 de febrero de 2020.
<b>OID (Identificación digital)</b>	<b>2.16.484.101.10.316.100.6.1.2.2.1</b>

Tabla 1 Identificación del documento

## Responsables

La siguiente tabla muestra las personas responsables directamente con la revisión y elaboración del documento, así como su firma autógrafa que valida su revisión.

<b>Cargo</b>	<b>Responsable</b>	<b>Firma</b>
<b>Líder y director de Proyecto</b>	Joaquín Alcántar Hernández.	
<b>Profesional Informático</b>	Ignacio Mota Cruz	
<b>Auxiliar de Apoyo Informático de Seguridad</b>	Marco Antonio Pacheco Alvarez	
<b>Profesional Jurídico</b>	Antonio Mendoza Laurel	

Tabla 2 responsables de revisión

## Autorización

La persona encargada de autorizar y dar el visto bueno del documento de Políticas de Constancias de Conservación de Mensajes de Datos es el Profesional Informático de Legalex GS.

<b>Cargo</b>	<b>Responsable del Vo. Bo.</b>	<b>Firma</b>
<b>Profesional Informático</b>	Ignacio Mota Cruz	

Tabla 3 Autorización

## Introducción

El presente documento contiene las *Políticas de Constancias de Conservación de Mensajes de Datos*, de la Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) Legalex GS S.A. de C.V., donde se establecen las reglas que se llevan a cabo para la prestación de servicios fiables de Constancias de Conservación de Mensajes de Datos.

Los servicios de Constancias de Conservación de Mensajes de Datos ofrecidos por Legalex GS están regidos por el Título Séptimo de las “*Reglas Generales a las que deben sujetarse los Prestadores de Servicios de Certificación*”, publicadas y actualizadas el 15 de mayo del 2018 por la Secretaría de Economía (SE) de los Estados Unidos Mexicanos; y cumplen con los estándares RFC 3161 conforme a lo estipulado en la NOM-151-SCFI-2016.

## Alcance

Este documento detalla los requerimientos que debe cumplir el servicio de la Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) de Legalex GS con respecto a la provisión y administración de Constancias de Conservación de Mensajes de Datos.

## Enfoque

El enfoque de una política de Constancias de Conservación de Mensajes de Datos es significativamente diferente de una declaración de práctica. Una política de Constancias de Conservación de Mensajes de Datos se define independientemente de los detalles específicos del entorno operativo específico de la ACCMD, mientras que una declaración de práctica se adapta a la estructura organizativa, los procedimientos operativos, las instalaciones y el entorno informático.

## Administración de cambios de las Políticas de Constancias de Conservación de Mensajes de Datos

Todas aquellas modificaciones que surtan efecto dentro de las *Políticas de Constancias de Conservación de Mensajes de Datos* y la *Declaración de prácticas de Constancias de Conservación de Mensajes de Datos* tendrán que seguir las siguientes reglas:

1. Poner a discusión los cambios que se quieran realizar y aclarar el porqué de estos.
2. Esperar la autorización de los cambios o las nuevas aportaciones por el Director Ejecutivo, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad.
3. Estructurar la nueva información y al incluirla, esperar por la aprobación del documento por el Director Ejecutivo, el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad. Una vez aceptados los cambios por este grupo hay que esperar la aprobación de los cambios por la Secretaría de Economía (Dirección General de Normatividad Mercantil).

4. No se realizarán cambios que no se puedan soportar tanto en lo teórico como en lo práctico.
5. Dar aviso a Secretaría de Economía de los cambios realizados.
6. Se hará público el documento con los cambios, solamente al personal autorizado y se actualizará la versión pública.

## Actores y entidades participantes en la infraestructura de la Emisión de Constancias de Conservación de Mensajes de Datos

Existen actores y entidades que participan dentro de la infraestructura de Emisión de Constancias de Conservación de Mensajes de Datos, cada uno de ellos desempeñan distintos roles durante el proceso de emisión de una constancia de conservación de mensajes de datos, los actores implicados son:

1. Una Autoridad Certificadora Raíz, en este caso la Secretaría de Economía (SE).
2. Un Prestador de Servicios de Certificación, siendo este Legalex GS.
  - o Una Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD), encargada del sistema de emisión o provisión y otros procesos relacionados con las Constancias de Conservación de Mensajes de Datos.
3. Los suscriptores o entidades finales, es decir, las personas u organizaciones que solicitarán el servicio de Emisión de Constancias de Conservación de Mensajes de Datos, que podrían también llamarse "solicitantes".
4. Parte que confía, son aquellos que expresan su "fe" en la Autoridad de Constancias de Conservación de Mensajes de Datos al creer que sus servicios son lo suficiente confiables. Por lo general, estos suelen ser también suscriptores.

## Conceptos generales

### Servicio de Emisión de Constancias de Conservación de Mensajes de Datos

Las Constancias de Conservación de Mensajes de Datos de Legalex GS están diseñados para probar que un mensaje de datos NO ha sido alterado o modificado a partir de la emisión de la citada constancia, con la finalidad principal de que puedan ser utilizados en contextos jurídicos y/o actos comerciales definidos en la normativa aplicable, serán provisionados para los siguientes objetivos:

- 1.- Proveer el servicio de Emisión de Constancias de Conservación de Mensajes de Datos de acuerdo con los estándares establecidos en la NOM-151-SCFI-2016.
- 2.- Garantizar que el mensaje de datos, respecto del cual se emitió una constancia de conservación, ha permanecido completo e inalterado desde el momento de la emisión de la constancia.



- 3.- Proveer el mecanismo que permita identificar si una Constancia de Conservación de Mensajes de Datos fue emitida por un Prestador de Servicios de Certificación acreditado.
- 4.- Validar que la constancia de conservación de Mensajes de Datos que ha sido emitida por un Prestador de Servicios de Certificación acreditado y que el contenido ha permanecido íntegro e inalterado tal y como se generó por primera vez en su forma definitiva.
- 5.- Brindar certeza jurídica, durante el periodo establecido en la normativa aplicable, a los mensajes de datos a los cuales les es aplicada una constancia de conservación.
- 6.- Proporcionar a los suscriptores o usuarios del servicio de Emisión de Constancias de Conservación de Mensajes de Datos y una disponibilidad de 24/7.

Los servicios que proveerá el PSC mediante la contratación de las Constancias de Conservación de Mensajes de Datos se dividen en los siguientes:

1. La provisión o emisión de Constancias de Conservación de Mensajes de Datos, este componente del servicio genera un token o identificador de transacción de la emisión de Constancias de Conservación de Mensajes de Datos.
2. Validación de la Constancias de Conservación de Mensajes de Datos, este componente es público y se encarga de validar que la Constancias de Conservación de Mensajes de Datos en un archivo es válido.

## **Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD)**

La autoridad emitirá Constancias de Conservación de Mensajes de Datos por transacción que el suscriptor o cliente final del servicio de Emisión de Constancias de Conservación de Mensajes de Datos realice. La ACCMD tiene la responsabilidad de prestar correctamente el servicio de emisión de Constancias de Conservación de Mensajes de Datos que se menciona en el apartado de servicios de emisión de Constancias de Conservación de Mensajes de Datos dentro de este documento.

La ACCMD es responsable de la operación de las transacciones que se crean y firman en nombre de la ACCMD y el suscriptor o receptor de la transacción. **[Visualizar contenido en la versión privada]**

El PSC cuenta con una unidad de Constancias de Conservación de Mensajes de Datos principal y su redundante. Cada unidad tiene una clave diferente, en el caso principal. El servicio administrado para las constancias de conservación de mensajes de datos se utiliza para asegurar que la ACCMD tenga comunicación en todo momento con la TSA.

## Suscriptores o Cliente

El suscriptor puede ser una persona física o moral que desean generar evidencia digital confiable a partir de un método que asocie datos o información con la hora obtenida desde de una fuente confiable y la firma de la ACCMD que lo emite. El conjunto de estos elementos permite demostrar que una serie de datos **no han sido alterados** desde un instante de tiempo específico y confiable, siempre y cuando cubra los requisitos para recibir el servicio de emisión de Constancias de Conservación de Mensajes de Datos, entre los cuales comprende:

1. Ser mayor de edad (18 años en los Estados Unidos Mexicanos).
2. Estar dado de alta ante el SAT con un RFC válido y vigente.
3. Ser suscriptor de Legalex GS.
4. Tener todos sus datos actualizados y haber firmado un contrato de prestación de servicios.

Otros aspectos importantes en esta política para los suscriptores son:

1. Cuando el suscriptor o cliente es una organización (personas morales en México), algunas de las obligaciones que se aplican a esa personal moral, deberán aplicarse también a los usuarios finales o sus representantes.
2. En caso de personales Morales, la organización, empresa o persona moral será responsable de hacer cumplir las obligaciones de los usuarios finales o representantes y las consecuencias que pueden tener de no cumplirlas, por lo tanto, se espera que la organización o empresa informe adecuadamente a sus usuarios finales.
3. La PSC mantendrá informado a los suscriptores o usuarios finales del servicio de las responsabilidades que se tendrán bajo esté servicio, así como, en caso de que la PSC sea suspendida o corrompa una ley, las acciones que llevará a cabo la PSC para subsanar el daño que pueda presentarse a sus suscriptores y clientes.
4. Cuando el suscriptor es un usuario final, el usuario final será considerado directamente responsable cuando sus obligaciones no se cumplan correctamente.

## Política de Constancias de Conservación de Mensajes de Datos

Legalex GS define los requisitos para la línea de las políticas de Constancias de Conservación de Mensajes de Datos para la ACCMD que utilizan un token o identificador, soporte para la clave pública de los certificados de Constancias de Conservación de Mensajes de Datos y respaldos de certificados de clave pública, con la precisión proporcionada por la TSA de Legalex GS.

### Identificación

**[Visualizar contenido en la versión privada]**

## Comunidad de usuarios y aplicabilidad

Esta política tiene como objetivo cumplir los requisitos para la firma electrónica para ser usada con la Constancias de Conservación de Mensajes de Datos o en su defecto los certificados que se utilizarán para el servicio de emisión de Constancias de Conservación de Mensajes de Datos. El tipo de certificado utilizado para el servicio de emisión de Constancias de Conservación de Mensajes de Datos se define en el RFC 3628, tema 5.3 “*User community and applicability*” así como en ETSI TS 101 733 v2.1.1 en su tema 4.4.1 “*Electronic signature with time (CAAdES-T)*” y 4.4.2 “*ES with complete validation Data References (CAAdES-C)*”. Así el cumplimiento de las normativas aplicables a la emisión de Constancias de Conservación de Mensajes de Datos como lo son las *Reglas generales a las que deben sujetarse los Prestadores de Servicios de Certificación*.

## Conformidad

Legalex GS reclamará la conformidad con el presente documento aplicado en las políticas de Constancias de Conservación de Mensajes de Datos identificando en los certificados digitales y en la emisión de Constancias de Conservación de Mensajes de Datos que se provean bajo la ACCMD **cumpliendo** con los siguientes requerimientos bajo la estandarización de la *ETSI TS 101 733 Anexo C, tema C.1 The signature Policy* y el *RFC 3628 tema 5.4 Conformance*, además, de contener los siguientes valores para la conformidad y aceptación de las mismas políticas:

1. Reclama la conformidad con la política de Constancias de Conservación de Mensajes de Datos identificada dentro del certificado o constancia que se emita bajo la ACCMD de Legalex GS que pone a disposición de los suscriptores o clientes y las partes que confían bajo petición, la evidencia para respaldar el reclamo de conformidad.
2. Las evidencias se pueden conformar por un informe de un auditor interno o externo a la organización de Legalex GS, previamente identificado, que confirme que la ACCMD cumple con los requisitos de las políticas de Constancias de Conservación de Mensajes de Datos. Así mismo el auditor no debe tener una relación jerárquica con el departamento que opera la ACCMD. Las auditorías deberán realizarse por un auditor independiente y competente, como se establece en la *RFC 3628, tema 5.4 Conformance*, inciso b.
3. La ACCMD conforme, demostrará que cumple con sus obligaciones tal y como se define en el título *Obligaciones de la ACCMD* de este mismo documento.
4. El PSC implementará los controles que cumplan con los requisitos de la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos.
5. Legalex GS puede emitir certificados de constancias de conservación para fines internos y de prueba, siempre y cuando los certificados no estén disponibles para otro uso, inclusive si Legalex GS se encuentra críticamente “no conforme”.

6. De no cumplir con lo establecido en la presente Política de Constancias de Conservación de Mensajes de Datos, ni los requisitos que se expiden a través del Código de Comercio y las Reglas Generales a las que deben sujetarse los PSC emitido por la Cámara de Diputados del H. Congreso de la Unión y la Secretaría de Economía respectivamente, Legalex GS dejará de proveer y administrar las constancias de conservación de mensajes de datos y sus servicios, hasta que haya demostrado lo contrario; Legalex GS tomará las medidas necesarias para remediar la “no conformidad” dentro de un periodo razonable.
7. El cumplimiento respecto a la ACCMD se verificará regularmente y cada vez que se realice un cambio importante en sus operaciones.

### **Ciclo de vida de las llaves.**

Legalex GS, como una ACCMD, se encargará de emitir, proveer y de administrar el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

El servicio de validación de las constancias de conservación de mensajes de datos, emitidas por Legalex GS será accesible desde el portal <https://www.legalexgs.com>; esto con la finalidad de verificar la validez y vigencia de la constancia emitida.

El sistema de ACCDM rechazará cualquier intento de emitir o proveer una Constancias de Conservación de Mensajes de Datos cuando el certificado de la ACCMD esté expirado o fuera de la vigencia.

### **Constancias de Conservación de Mensajes de Datos**

El sistema ACCMD de Legalex GS cumplirá con los estándares señalados en el RFC 3161 para garantizar la calidad, el rendimiento y el funcionamiento del servicio de emisión de Constancias de Conservación de Mensajes de Datos.

El sistema ACCMD de Legalex GS utiliza un algoritmo SHA-2 de 256 bits bajo los estándares divulgados en FIPS PUB 180-4 (NIST, 2018) que cumplen los estándares necesarios para llevar a cabo el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

### **Estructura de las Constancias de Conservación de Mensajes de Datos**

Las Constancias de Conservación de Mensajes de Datos emitidas por la ACCMD de Legalex GS deben cumplir con las especificaciones técnicas del estándar RFC 3161 (IETF, 2018).

La estructura de la Constancias de Conservación de Mensajes de Datos (Token de Constancias de Conservación de Mensajes de Datos) contiene los siguientes elementos:

1. Un identificador de la política de la ACCMD.

2. Un número de serie único que permita identificar una Constancias de Conservación de Mensajes de Datos específico.
3. El tiempo, fecha y hora de generación, indicando la fuente de tiempo confiable.
4. La representación del dato (Hash), provisto por el suscriptor al cual le será emitida la constancia de conservación.
5. La firma electrónica que ha sido generada usando una llave pública de la ACCMD.
6. La identificación de la ACCMD.

Para más información consulte la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos.

### Algoritmo de encriptación de datos

El sistema ACCMD de Legalex GS utiliza un algoritmo SHA-2 de 256 bits bajo los estándares divulgados en FIPS PUB 180-4 (NIST, 2018) que cumplen los estándares necesarios para llevar a cabo el servicio de emisión de Constancias de Conservación de Mensajes de Datos. **[Visualizar contenido en la versión privada]**

## Obligaciones y responsabilidades

### Obligaciones

#### Obligaciones del PSC

La PSC de Legalex GS, se asegurará de que todos los procedimientos detallados en la Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos se lleven a cabo. El PSC también garantizará el cumplimiento de cualquier obligación adicional indicada en el servicio de Constancias de Conservación de Mensajes de Datos, ya sea directamente o incorporada por referencia. Otras obligaciones a las que está sujeta el PSC son:

1. Proporcionar el servicio de emisión de Constancias de Conservación de Mensajes de Datos de acuerdo con su declaración de práctica y la presente Política de Constancias de Conservación de Mensajes de Datos.
2. Usar, establecer y crear sistemas o plataformas que sean lo suficientemente seguros y confiables, que estén protegidos contra terceras personas no autorizadas y accesos no deseados, contemplando la seguridad de hardware y de software, y las técnicas de encriptación que se deban utilizar para evitar ataques informáticos no deseados.
3. Garantizar que los servicios de la ACCMD sean ofrecidos mediante un sitio de alta disponibilidad.
4. Garantizar que la ACCMD mantenga comunicación permanente con la TSA para el consumo de los sellos de tiempo que integran la constancia.

5. Garantizar que las Constancias de Conservación de Mensajes de Datos emitidas estarán correctamente conformadas y permitirán determinar la validez de la misma.
6. Mantener un control del personal de Legalex GS asociado al servicio, y en caso de requerir un prospecto, los candidatos, mantengan el perfil deseado en base a los criterios de calificación, conocimientos, experiencia medible mediante exámenes o simulacros de ejercicios, sobre todo para los servicios que involucran la emisión de Constancias de Conservación de Mensajes de Datos, infraestructura de redes, seguridad, auditorías internas y cualquier otro necesario, tal como lo establecen las Reglas Generales a las que deberán sujetarse los prestadores de servicios de certificación.
7. Determinar el control del mantenimiento y la aplicación de la infraestructura tanto de hardware (operacional) como de software, sobre los servicios de emisión de Constancias de Conservación de Mensajes de Datos.
8. Realizar una revisión anual del presente documento y en su caso, realizar las actualizaciones necesarias con la aprobación requerida.
9. Garantizar a través de auditorías, tanto internas como externas, que Legalex GS cumple con todos los requerimientos establecidos por la SE, para obtener la acreditación como Prestador de Servicios de Certificación en el servicio de emisión de Constancias de Conservación de Mensajes de Datos.
10. Poner a disposición de los usuarios la Política de Constancias de Conservación de Mensajes de Datos Pública, así como la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos pública en el sitio <https://www.legalexgs.com>.
11. Atender las inconformidades de los suscriptores, clientes y terceros de confianza, según lo pactado en los términos y condiciones del contrato de servicios, incluyendo la disponibilidad y alcance del servicio que Legalex GS que estará prestando.
12. Definir sus propias políticas para mejorar el servicio o restringir el mal uso que se le dé al servicio de emisión de Constancias de Conservación de Mensajes de Datos.

Para ver el listado completo de las obligaciones del PSC dirigirse a la declaración de prácticas de SDT en el tema Obligaciones y responsabilidades, subtema Obligaciones del PSC.

### **Obligaciones de los Suscriptores o Clientes**

Los términos, condiciones, uso y prácticas legales del servicio de emisión de Constancias de Conservación de Mensajes de Datos se encuentran detallados dentro del contrato de servicios de Legalex GS, donde se marcan las obligaciones de los suscriptores o clientes hacia el PSC y el uso de las Constancias de Conservación de Mensajes de Datos, entre las cuales se encuentran:

1. Conocer, entender y aceptar las Políticas y la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos de Legalex GS.

2. Conocer el propósito y el alcance de las Constancias de Conservación de Mensajes de Datos emitidos o proveídos por Legalex GS y usarlo únicamente para lo estipulado en la presente Política de Constancias de Conservación de Mensajes de Datos.
3. En su caso, aceptar los términos y condiciones que le plantee Legalex GS.
4. Solicitar Constancias de Conservación de Mensajes de Datos únicamente desde las plataformas autorizadas por Legalex GS.
5. Verificar que el token recibido por parte del servicio de Constancias de Conservación de Mensajes de Datos contenga los elementos necesarios y que el certificado de la PSC expedido por la SE que firmó dicho token o identificador se encuentre vigente.
6. No modificar o intentar modificar los tokens o identificadores de Constancias de Conservación de Mensajes de Datos emitidos por la ACCMD.

Para ver el listado completo de las obligaciones de los suscriptores dirigirse a la declaración de prácticas de certificación en el tema Obligaciones y responsabilidades, subtema Obligaciones de los suscriptores.

### **Obligaciones de la parte que confía**

Las personas u organizaciones que confíen en las Constancias de Conservación de Mensajes de Datos de Legalex GS se atenderán a los términos y condiciones de la ACCMD las cuales estipulan:

1. Verificar que el token recibido por parte del servicio de Constancias de Conservación de Mensajes de Datos contenga los elementos necesarios y que el certificado de la PSC expedido por la SE que firmó dicho token o identificador, se encuentre vigente.
2. Conocer el propósito y el alcance de las Constancias de Conservación de Mensajes de Datos emitidos por Legalex GS y usarlo únicamente para lo estipulado en la presente política de Constancias de Conservación de Mensajes de Datos.
3. Asegurar el uso de las Constancias de Conservación de Mensajes de Datos, para los usos estipulados en el presente documento.
4. Notificar o dar aviso sobre cualquier situación considerada anómala con respecto a los servicios de Constancias de Conservación de Mensajes de Datos y/o a constancias de conservación emitidas o proveídas.

### **Responsabilidades del PSC**

1. Garantizar el cumplimiento de las obligaciones descritas en el anterior segmento y de verificar la correcta aplicación por parte de los involucrados, y aplicar lo correspondiente, en los supuestos de incumplimiento.
2. Al aplicar alguna sanción, en caso de que exista, se debe actuar con efectividad y de forma profesional a las tareas y obligaciones que fueron

- quebrantadas, presentándolas con los superiores (Director Ejecutivo, Profesional Informático y Profesional Jurídico).
3. Asegurar que las Constancias de Conservación de Mensajes de Datos que expida Legalex GS son válidas y mantienen la estructura que se declara en este documento.
  4. El token o identificador de Constancias de Conservación de Mensajes de Datos, es único y va en respuesta a una sola solicitud de parte del suscriptor o cliente.

### Responsabilidades de los suscriptores o clientes

1. Resguardar los archivos que se entregan a efecto de cada constancia de conservación y de administrar sus propias copias de seguridad de los archivos respecto de los cuales se realice la emisión.
2. Mantener un uso correcto de sus credenciales para el servicio de ACCMD, de no ser así, el uso que le den otras personas será bajo responsabilidad del suscriptor, de acuerdo con el Código de Comercio Artículo 21.
3. Asegurarse que los datos que proporcione para la creación de sus credenciales de acceso y la firma del contrato de servicios se hayan asentado correctamente, ya que las declaraciones que haga el suscriptor o cliente se tomarán como verdaderas y cualquier dato falso podría ser causa de una penalización severa según la ley aplicable.

Para ver el listado completo de las responsabilidades de los suscriptores o clientes dirigirse a la declaración de prácticas de ACCMD en el tema Responsabilidades de los suscriptores o clientes.

### Descarto de responsabilidades

Mediante la *Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos*, se obtiene que Legalex GS, S.A. DE C.V. no tendrá ni asumirá ninguna responsabilidad o compromiso cuando ocurra alguna de las situaciones expresadas en el documento, dentro de las limitaciones de Responsabilidad y limitaciones del servicio. Para más información consultar la Declaración de prácticas de ACCMD en el tema Descarto de Responsabilidades.

### Limitaciones del servicio

El servicio de emisión de Constancias de Conservación de Mensajes de Datos de Legalex GS solo se proporcionará a los suscriptores que tengan un contrato de servicio con Legalex GS. Dicho servicio se puede solicitar en conjunto con cualquier otro servicio que proporciona el PSC.

El PSC se reserva la responsabilidad de garantizar la validez de un token o identificador de Constancias de Conservación de Mensajes de Datos más allá del final del período de validez del certificado emitido para la ACCMD.



### **Responsabilidades Económicas**

Las responsabilidades económicas respecto de la ACCMD de Legalex GS se visualizan específicamente con las indemnizaciones que debe realizar el PSC hacia la AC Raíz (Secretaría de Economía) o los suscriptores o clientes cuando se exhibe una irresponsabilidad. Para más información consulte el Tema de Responsabilidades Económicas dentro de la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos.

### **Términos y condiciones**

Legalex GS pondrá a disposición del público en general un documento de "Términos y condiciones", en el cual se encontrará información sobre la limitación del servicio, las obligaciones de los suscriptores, la información para las partes que confían o las limitaciones de responsabilidad, entre otros. Dicho documento puede ser consultado dentro del contrato de prestación del servicio de forma puntual.

## Anexos

### Apéndice A

#### Acrónimos

Abreviaciones más comunes que se pueden encontrar dentro de este documento:

Acrónimo	Significado
<b>ACCMD</b>	Autoridad de Constancias de Conservación de Mensajes de Datos.
<b>ETSI</b>	Instituto europeo de Normas de telecomunicaciones (European telecommunications standards institute), es una organización de estandarización independiente, que entre sus protocolos conforma el uso de redes fijas y de convergencia (internet). (ETSI, 2017)
<b>FIPS 140-2</b>	Federal information processing standard, Estándares federales de procesamiento de la información. Es un estándar de seguridad de ordenadores para la acreditación de módulos criptográficos. (NIST, National Institute of Standards and Technology, 2001)
<b>HSM</b>	Hardware security module, Módulo de seguridad de Hardware. El HSM es un dispositivo criptográfico basado en hardware que genera, almacena y protege claves criptográficas y suele aportar aceleración de hardware para operaciones criptográficas de seguridad. (Safenet, 2015)
<b>IETF</b>	Grupo de trabajo en ingeniería de internet (Internet engineering task force), organismo que produce reglamentos y/o estándares para la producción de alta calidad sobre protocolos y uso de la internet. (IETF, 2015)
<b>ITU-T</b>	Siglas del Sector de Normalización de las Telecomunicaciones de la Unión de telecomunicaciones. (ITU, 2017)
<b>NIST</b>	Acrónimo de National Institute of Standards and Technology. (NIST, National Institute of Standards and Technology, 2001)
<b>NTP</b>	Acrónimo de Network Time Protocol, Es el protocolo que se utiliza para sincronizar los relojes de los sistemas informáticos. (Wikipedia, 2018)
<b>NTPD</b>	Network Time Protocol Daemon.
<b>PSC</b>	Prestador de Servicios de Certificación, hace referencia a la persona o institución pública que presta los servicios relacionados con sellos digitales de tiempo, firma electrónica, conservación de mensajes de datos y digitalización. (Secretaría de Economía, 2007)
<b>RFC</b>	Acrónimo de <i>Request for comments</i> , que no es más que una serie de publicaciones que hacen a través de internet mediante la IETF (Engineering Task Force). (IETF, 2015)
<b>SE o S.E.</b>	Secretaría de Economía
<b>TSA</b>	Autoridad de sellado de tiempo (RFC 3628, 2018)
<b>UTC</b>	Tiempo Universal Coordinado

Tabla 4 Acrónimos

**Glosario**

Definición	Significado
<b>Firma electrónica</b>	Es utilizada para identificar al firmante en relación con los mensajes de datos y llaves criptográficas e indicar que el firmante aprueba la información contenida en el mensaje de datos que quiere validar, es decir, al ser validada con una firma electrónica, este documento o mensaje validado cuenta para efectos jurídicos, como cualquier firma autógrafa. (Secretaría de Gobernación SEGOB, 2012)
<b>Llave privada</b>	Datos que el firmante genera de manera secreta y utiliza para crear su firma electrónica avanzada, a fin de lograr el vínculo entre dicha firma electrónica avanzada y el firmante. (Secretaría de Gobernación SEGOB, 2012)
<b>Llave pública</b>	Son llaves criptográficas, datos, códigos o registros únicos que utiliza un destinatario para verificar la autenticidad de la firma electrónica del firmante. (RedHat INC, 2017)
<b>Middleware</b>	Software que se sitúa entre un sistema operativo y las aplicaciones que se ejecutan en él. Básicamente, funciona como una capa de traducción oculta para permitir la comunicación y la administración de datos en aplicaciones distribuidas. (Microsoft azure, 2012)
<b>Parte que confía</b>	Hace referencia a la persona que siendo o no el Destinatario, actúa sobre la base de un certificado o una firma electrónica, incluyendo cualquier otro servicio brindado por una PSC. (Secretaría de Economía, 2008)
<b>Suscriptor</b>	Se entiende por suscriptor, toda aquella persona física o moral que es titular de un servicio proporcionado por la PSC de Legalex GS, donde voluntariamente confía y hace uso de los servicios.
<b>Web Service</b>	El término Web Services describe una forma estandarizada de integrar aplicaciones WEB mediante el uso de XML, SOAP, WSDL y UDDI sobre los protocolos de la Internet. (C, 2006)

Tabla 5 Definiciones

## Apéndice B

### Bibliografía

[Visualizar contenido en la versión privada]