LEGALEX GS®

DECLARACIÓN DE PRÁCTICAS

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: 2.16.484.101.10.316.100.6.1.2.2.1

VERSIÓN PÚBLICA

Esto es una versión pública y no contiene todo el material completo de la Declaración de prácticas de las 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.

DECLARACIÓN DE PRÁCTICAS DE CONSTANCIAS DE CONSERVACION DE MENSAJES DE DATOS

LEGALEX GS, S.A. DE C.V.

OID: 2.16.484.101.10.316.100.6.1.2.2.1

LEGALEX GS S.A. DE C.V.

LGS160502EA8

LEGALEX GS S.A. DE C.V.

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

Fecha de inicio de operaciones como PSC para el servicio de Constancias de Conservación de Mensajes de Datos: 16 DE OCTUBRE DEL 2020

Tabla de contenido

Identificación del documento 5
Responsables 5
Autorización 6
Presentación del PSC 7
Misión 7
Visión 7
Objetivos 8
Introducción 8
Alcance 9
Conceptos generales 9
Servicios de las Constancias de Conservación de Mensajes de Datos 9
Interacción de los servicios 10
Entidades participantes en la infraestructura de Constancias de Conservación de Mensajes de Datos 13
Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) 14
Suscriptores 14
Requisitos de las prácticas de la PSC. 15
Declaración de prácticas y divulgación de la ACCMD 15
Declaración de prácticas de la ACCMD 15
Declaración de divulgación del PSC 16
Gestión del ciclo de vida de las llaves 17
Generación de las Claves de la ACCMD 17
Protección de claves. 18
Distribución de la clave pública de la ACCMD 18
Renovación (nueva emisión) de las claves de la ACCMD 18
Fin del ciclo de vida de las claves de la ACCMD 19
Gestión del ciclo de vida del módulo criptográfico usado para las Constancias de Conservación de Mensajes de Datos 19
Sobre el servicio de Constancias de Conservación de Mensajes de Datos 19
Token o identificador de Constancias de Conservación de Mensajes de Datos 19
Vigencia de la Constancia de Conservación de Mensajes de Datos 19
Gestión y operación del CCMD 19
Requerimientos para operar el servicio 19
Clasificación y gestión de activos 20

Solicitud de servicio 21
Gestión y clasificación de los activos 21
Seguridad del personal 21
Proceso de Reclutamiento 21
Seguridad física y ambiental 21
Gestión de operaciones 22
Gestión de acceso a los sistemas 22
Mantenimiento e implementación de sistemas de confianza 22
Compromiso de los servicios del PSC 22
Terminación y Sucesión de la ACCMD 22
Cumplimiento de requerimientos legales 24
Registro de información concerniente a las operaciones del servicio de emisión de Constancias de Conservación de Mensajes de Datos 24
Obligaciones y responsabilidades 24
Obligaciones 24
Obligaciones del PSC 24
Obligaciones de los Suscriptores 26
Obligaciones de la parte que confía 27
Responsabilidades 27
Responsabilidades de la PSC. 27
Responsabilidad de los suscriptores 28
Limitaciones de la Responsabilidad 28
Descarto de responsabilidades 29
Restricciones de uso de las Constancias de Conservación de Mensajes de Datos 29
Responsabilidades Económicas 29
Términos y condiciones 30
Políticas de Constancias de Conservación de Mensajes de Datos 30
Identificación 30
Comunidad de usuarios y aplicabilidad 30
Conformidad 31
Aplicabilidad 32
Organización 32
Consideraciones de seguridad 33
Auditorías 33
Anexos 34

Apéndice A....34
Acrónimos....34
Definiciones....36
Apéndice B....37

Tabla de cuadros y esquemas

Tabla 1 Identificación del documento 5
Tabla 2Responsables 5
Tabla 3Autorización 6
Tabla 5Acrónimos 35
Tabla 6 Glosario de definiciones 37

Tabla de ilustraciones

Ilustración 3 Escalonamiento de la ACCMD 14

Identificación del documento

En esta sección se identifican los datos principales del documento:

Nombre	Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos
Versión	**1.2 PÚBLICA**
Autor	Legalex GS.
Estado	Actualizado
Fecha de elaboración	30 de junio de 2019.
Fecha de actualización	03 de febrero de 2020.
OID (Identificador digital)	2.16.484.101.10.316.100.6.1.2.2.1

Tabla 1 Identificación del documento

Responsables

En la siguiente tabla se muestran las personas responsables directamente con la revisión y elaboración del documento.

Cargo	Responsable	Firmas
Líder y Director Ejecutivo	Joaquín Alcántar Hernández	
Profesional Informático	Ignacio Mota Cruz	
Auxiliar de Apoyo Informático de Seguridad	Marco Antonio Pacheco Alvarez	
Profesional Jurídico	Antonio Mendoza Laurel	

Tabla 2Responsables

Autorización

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

Cargo	Responsable del Vo. Bo.	Firma
Profesional Informático	Ignacio Mota Cruz	

Tabla 3Autorización

Presentación del PSC

Legalex GS es un órgano interlocutor entre las personas que necesitan el uso de las Constancias de Conservación de Mensajes de Datos frente al sector público y privado. Además de promover el uso de los medios electrónicos/digitales en la colaboración entre empresas y personas, usando siempre las mejores prácticas y estándares de calidad en la prestación de sus servicios.

Ser un Prestador de Servicios de Certificación (PSC), significa obtener la acreditación otorgada por la Secretaría de Economía, teniendo la función de proveer y administrar las Constancias de Conservación de Mensajes de Datos, en conjunto con los términos y los requisitos que establece el Código de Comercio y las Reglas Generales a las que deberán sujetarse los PSC, con el fin de que todas las constancias que sean otorgados creen certeza jurídica y seguridad informática tanto de los datos personales como en los actos de comercio por medios electrónicos o digitales (plataformas móviles, internet, dispositivos digitales).

Así mismo, una PSC está obligada a otorgar el reconocimiento jurídico en todos sus servicios y medios electrónicos que sean extraídos, determinar los alcances que tendrá el contenido de las Constancias de Conservación de Mensajes de Datos sobre todo en el ámbito público y en los medios electrónicos que la puedan conformar donde se tendrán que reconocer los medios de prueba, es decir, la prueba sobre los mensajes y la conservación de estos como los datos.

La Declaración de prácticas de Constancias de Conservación de Mensajes de Datos es autorizada por el Director Ejecutivo, el Profesional Informático, el Auxiliar de Apoyo Informático de Seguridad y el Profesional Jurídico.

Por ende, se asume que al continuar leyendo el documento el lector tendrá el conocimiento básico y entenderá los conceptos que se manejan en el documento, como lo son la infraestructura de la Clave pública, el concepto de la emisión o provisión de las Constancias de Conservación de Mensajes de Datos y lo que esto implica, esquematizando en consecuencia los componentes generales involucrados en la infraestructura de Clave pública.

Misión

Nuestra misión es ser una empresa prestadora de servicios de Constancias de Conservación de Mensajes de Datos eficiente y competitiva a nivel mundial. Caracterizada por su creatividad, solidez, eficiencia y honestidad. Centrados en la satisfacción oportuna de las necesidades de nuestros clientes.

Visión

Consolidarnos como la mejor empresa prestadora de servicios de certificación siendo innovadores en los servicios financieros y tecnológicos, buscando siempre estar a la vanguardia del mercado.

Objetivos

Identificar, evaluar y valorar las prácticas que se debe presentar en las oficinas centrales, donde se desarrollan los principales procedimientos de la empresa Legalex GS; con el fin de priorizar y establecer controles necesarios para el desarrollo de las Constancias de Conservación de Mensajes de Datos y sus servicios, mantener la seguridad tanto del personal que labora como de los datos sensibles que se manejan y proveer la estructura organizacional que presenta la ACCMD.

Introducción

El presente documento contiene la *Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos*, de la Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) Legalex GS donde se establecen términos y condiciones, así como las prácticas comerciales y operativas para llevar a cabo la prestación de servicios fiables de Constancias de Conservación de Mensajes de Datos.

La declaración de práctica de Constancias de Conservación de Mensajes de Datos es más específica que una política de Constancias de Conservación de Mensajes de Datos. Una declaración de práctica de CCMD es una descripción más detallada de los términos y condiciones, así como las prácticas comerciales y operativas de una ACCMD en la emisión o provisión y administración de servicios de Constancias de Conservación de Mensajes de Datos. La declaración de práctica de CCMD de una PSC impone las reglas establecidas por una política de marca de tiempo. Una declaración de práctica de CCMD, define como una ACCMD cumple con los requisitos técnicos, organizativos y de procedimiento identificados en una política de Constancias de Conservación de Mensajes de Datos.

El servicio de Emisión de Constancias de Conservación de Mensajes de Datos ofrecidos por Legalex GS están regidos por *las* Reglas Generales a las que deberán sujetarse los Prestadores de Servicios de Certificación y cumplen con los estándares RFC 3161 *"Time-Stamp Protocol (TSP),"* así como el uso de una de las extensiones señaladas en el RFC 5280.

En general, en este documento, detalla un conjunto de disposiciones las cuales implican:

1. Los procedimientos de operación para otorgar y proveer una constancia de conservación de mensajes de datos y el alcance de estas.
2. Las responsabilidades y obligaciones del PSC, suscriptores y terceros de confianza.
3. Las medidas de seguridad adoptadas para proteger los datos de creación de firma electrónica para Constancias de Conservación de Mensajes de Datos.
4. Controles que se utilizarán para asegurar las auditorías y el almacenamiento de información relevante.
5. Compatibilidad con el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280.

6. Parte de esta declaración será pública.

Alcance

Este documento detalla las normas, condiciones, estructura organizativa, los procedimientos operativos, las responsabilidades, obligaciones medidas de seguridad para las instalaciones y el entorno informático de la ACCMD de Legalex GS con respecto al servicio de emisión y validación de Constancias de Conservación de Mensajes de Datos.

Conceptos generales

Servicios de las Constancias de Conservación de Mensajes de Datos

Las Constancias de Conservación de Mensajes de Datos de Legalex GS están diseñados para probar que un dato no ha sido alterado o modificado a partir de la emisión de la constancia de conservación 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 ha sido emitida por un Prestador de Servicios de Certificación acreditado y que el contenido ha permanecido integro 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 del servicio de Emisión de Constancias de Conservación de Mensajes de Datos con una disponibilidad 24/7.

Los servicios que proveerá la PSC mediante la contratación del servicio de emisión de 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 Constancia de Conservación de Mensajes de Datos.

2. Validación de la Constancia de Conservación de Mensajes de Datos, este componente es público y se encarga de validar que las Constancias de Conservación de Mensajes de Datos en un archivo es válido.

Interacción de los servicios

Emisión o provisión de Constancias de Conservación de Mensajes de Datos

Actualmente en la PSC Legalex GS, contemplamos dos esquemas para el consumo del servicio de Emisión de Constancias de Conservación de Mensajes de Datos, los cuales constan de:

- Peticiones cliente a cliente.
- Uso de nuestra plataforma (consumo de la CCMD mediante el cliente de la ACCMD).

Petición cliente-cliente

Las Constancias de Conservación de Mensajes de Datos cliente-cliente consta que una aplicación cliente externa al aplicativo cliente de la ACCMD Legalex, se conecta al servicio y hace peticiones tipo *.TSQ, sin que intervengan las interfaces del propio aplicativo de la ACCMD que administra las peticiones (Legalex ACCMD, el proceso de emisión de Constancias de Conservación de Mensajes de Datos se efectúa de la siguiente manera:

1. Cotizar el servicio a través del Director Ejecutivo.
2. Entregar documentación requerida (razón social, RFC, pagos, copias de identificaciones oficiales) y celebrar el contrato de servicios sobre Constancias de Conservación de Mensajes de Datos correspondiente, donde el suscriptor firma de conformidad del servicio y nuestros términos y condiciones.
3. Guardar y cuidar las credenciales, así como las plantillas de acceso, que se le proporcionen para el uso del servicio de CCMD.
4. Una vez establecidas las conexiones entre el sistema del cliente y el cliente de la ACCMD de Legalex GS, realizar las pruebas correspondientes.
5. Al efectuarse la petición del servicio de Emisión de Constancias de Conservación de Mensajes de Datos, se hace la petición a la ACCMD de Legalex GS para la emisión de constancias.
    a. Una vez que la ACCMD recibe la petición de emisión de la constancia, esta a su vez solicita a la TSA de Legalex GS la emisión del Sello Digital de Tiempo correspondiente.
6. Durante el proceso de la CCMD regresa un objeto tipo token, el cual contiene la siguiente información:
    a. Número entero que corresponde al serial o identificador de la constancia.
    b. Hash de la constancia de conservación.
    c. Hora y fecha en la que se emitió la constancia.
    d. Información de la ACCMD que emite la constancia.

7. Una vez terminado el proceso de ACCMD, el middleware regresa el resultado final del documento del cual se emitió la constancia de conservación, en conjunto con tres archivos que son el respaldo de que la operación fue exitosa. Estos archivos son:
    a. ***.LTSR** (TimeStampRequest), este archivo contiene la respuesta de la CCMD.
    b. ***.LTSQ** (TimeStampQuery), este archivo contiene el hash del documento del cual se emitió la constancia de conservación.
    c. ***.PDF**, como representación gráfica de la constancia que acaba de ser emitida.
8. Una vez terminado el proceso emisión de la constancia se devuelve el resultado de la petición a la aplicación cliente que la solicitó.
9. Cuando termine la operación, la aplicación cliente de la ACCMD actualiza a la redundancia.

Cabe mencionar que cada aplicativo de cliente externo a Legalex GS, se le mandarán los archivos ***.LTSR, *.LTSQ y *.PDF** como resultado de la solicitud de Emisión de una Constancia de Conservación de Mensajes de Datos. El desarrollador del aplicativo cliente se responsabilizará de hacerle llegar estos archivos a su cliente final o utilizarlos según sus propias políticas.

Emisión de la CCMD mediante el cliente de la ACCMD

La provisión de las Constancias de Conservación de Mensajes de Datos también se podrá realizar mediante un aplicativo cliente que se conecta directamente a la ACCMD de Legalex GS, donde los clientes o suscriptores podrán acceder una vez que tengan sus credenciales de acceso, en la cual podrán subir el archivo que desean aplicar la CCMD y en ese mismo sitio podrán descargar el resultado de la operación de la CCMD, teniendo los siguientes pasos a realizar:

1. Cotizar del servicio a través del Director Ejecutivo.
2. Entregar la documentación requerida (razón social, RFC, pagos, copias de identificaciones oficiales) y celebrar el contrato de servicios sobre las Constancias de Conservación de Mensajes de Datos correspondiente, donde el suscriptor firma de conformidad del servicio y nuestros términos y condiciones.
3. Guardar y cuidar las credenciales de acceso que se le den para comenzar el uso del servicio de CCMD.
4. Acceder a la plataforma o sitio web donde podrá realizar las operaciones de Constancias de Conservación de Mensajes de Datos https://www.legalexgs.com/legalex_nom/ subir los archivos respecto de los cuales se emitirá constancia y hacer la petición de emisión de constancia de conservación de mensajes de datos una vez terminado de subir los archivos.
5. Una vez realizada la petición esta viajará hasta ser recibida por la ACCMD quien será la encargada de emitir la CCMD.

   a. Una vez que la ACCMD recibe la petición de emisión de la constancia, esta a su vez solicita a la TSA de Legalex GS la emisión del Sello Digital de Tiempo correspondiente.
6. Sí estas peticiones son correctas, se hace la solicitud de la CCMD a la ACCMD la cual se encargará de firmar la petición, extrayendo las llaves del HSM para firmar la petición con el certificado de Constancias de Conservación de Mensajes de Datos de la ACCMD dentro del HSM.
7. Una vez terminado el proceso de CCMD el middleware regresa el resultado final del documento respecto del cual se emitió constancia en conjunto con tres archivos que son el respaldo de que la operación fue exitosa al aplicativo cliente de la ACCMD, estos archivos son:
   a. ***.LTSR** (TimeStampRequest), este archivo contiene la respuesta de la CCMD.
   b. ***.LTSQ** (TimeStampQuery), este archivo contiene el hash del documento del cual se emitió la constancia de conservación.
   c. ***.PDF**, como representación gráfica de la constancia que acaba de ser emitida.
8. La constancia de conservación queda almacenada la operación en la base de datos del cliente de la ACCMD. Estos archivos son recibidos y almacenados dentro del cliente de la ACCMD, registrando la operación y los archivos originales en conjunto de los respaldos de operación de la CCMD.
9. El cliente o suscriptor final obtiene, descarga y visualiza su petición ya con la constancia en conjunto con sus respaldos.

Validación de la CCMD

La validación de la CCMD se realiza a través de la página de Legalex GS, entrando a la siguiente URL que se encuentra disponible de forma pública: https://www.legalexgs.com/Servicios/sellos/validarNOM.jsp donde los clientes o suscriptores finales tendrán que seguir los siguientes pasos:

1. El suscriptor deberá subir el archivo original y el archivo que respalda la CCMD (archivo Legalex).
2. Una vez que el suscriptor haya cargado los archivos, se ejecuta una función de validación en la cual se provee el certificado de emisión de la ACCMD, los tres archivos que subió el suscriptor y la librería desarrollada para java de open source (Bouncy castle) determinan si es válido o no.
3. Bouncy castle verifica la firma de la ACCMD, valida que el certificado sea el mismo con el que fue emitida la constancia y así mismo el hash de la CCMD en relación con el documento original.

El resultado se presenta ante el suscriptor mediante el sitio web público, desplegando si el archivo que fue cargado por el suscriptor sigue siendo válido o no, así mismo muestra el archivo original para el cotejo del suscriptor.

Entidades participantes en la infraestructura de Constancias de Conservación de Mensajes de Datos

Existen actores y entidades que participan dentro de la infraestructura de Constancias de Conservación de Mensajes de Datos, cada uno de ellos desempeñan distintos roles durante el proceso de emisión de una Constancias 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.
    a. 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 las Constancias de Conservación de Mensajes de Datos, a los que llamaremos "solicitantes".
4. Terceros que confían, son aquellos que expresan su "fe" en la Autoridad de Constancias de Conservación de Mensajes de Datos al creer que sus servicios son lo suficientemente confiables. Por lo general, estos suelen ser también subscriptores, pero no necesariamente debe ser así.

Ilustración 1 Escalonamiento de la ACCMD

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

La autoridad emitirá Constancias de Conservación de Mensajes de Datos por cada transacción realizada por el suscriptor o cliente final del servicio de emisión de Constancias de Conservación de Mensajes de Datos. La ACCMD tiene la responsabilidad de llevar a cabo correctamente el servicio de Emisión de Constancias de Conservación de Mensajes de Datos que se nombran en el tema *Servicios de emisión de Constancias de Conservación de Mensajes de Datos* dentro de este documento.

La ACCMD es responsable de la operación de la unidad de Constancias de Conservación de Mensajes de Datos, es decir, las transacciones que se crean y firman en nombre de la ACCMD y el suscriptor o receptor de la transacción. La ACCMD es responsable de emitir Constancias de Conservación de Mensajes de Datos las cuales están configuradas para incluir un sello digital de tiempo, el cual obtendrán a través de la TSA de Legalex GS.

Suscriptores

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 un documento no ha sido alterado en el tiempo y conserva la forma definitiva con la cual fue generado por primera vez, siempre y cuando cumpla los requisitos para hacer uso del servicio de Constancias de Conservación de Mensajes de Datos, entre los cuales comprende:

1. Ser mayor de edad (18 años en los Estados Unidos Mexicanos) o ser una sociedad legalmente constituida.
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 entre las políticas para los suscriptores recaen en:

1. Cuando el suscriptor 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. El 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.

Requisitos de las prácticas de la PSC.

La PSC implementa controles para cumplir con los requisitos del servicio de emisión de Constancias de Conservación de Mensajes de Datos. Estos requisitos no implican alguna restricción para ofrecer los servicios de la ACCMD.

La provisión de un token o identificador de una Constancia de Conservación de Mensajes de Datos en respuesta a una solicitud queda a moderación de la PSC según los acuerdos de nivel de servicio que se establecen en la política de CCMD y en el presente documento.

Declaración de prácticas y divulgación de la ACCMD

Declaración de prácticas de la ACCMD

Dentro de la Declaración de prácticas de CCMD, el PSC se asegura que se demuestra la integridad necesaria para proporcionar el servicio de emisión de Constancias de Conservación de Mensajes de Datos. En particular se describe lo siguiente:

1. El PSC expone ante la SE el documento de Análisis y Evaluación de Riesgos y Amenazas tal y como se especifican en la **Regla 144** de las Reglas Generales a las que deberán sujetarse los PSC. Dicho documento especifica las vulnerabilidades que pueden afectar a los activos de la ACCMD y como se debe actuar en caso de ocurrir una amenaza.
2. El PSC expone su declaración de prácticas y procedimientos en el documento *Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos.* El cual aborda los requisitos para ofrecer los servicios, según la **Regla 163** de las Reglas Generales a las que deberán sujetarse los PSC.
3. La declaración de prácticas establece las obligaciones de las organizaciones externas que brindan apoyo al PSC. Así mismo las políticas de seguridad de la información establecen controles para la contratación de estas.
4. Legalex GS a través de su portal electrónico pondrá a disposición de los suscriptores y las partes que confían, su declaración de práctica de CCMD y sus políticas de Constancias de Conservación de Mensajes de Datos, para evaluar el cumplimiento de las políticas de Constancias de Conservación de Mensajes de Datos como se especifica en la **Regla 161** de las Reglas Generales a las que deberán sujetarse los PSC.
5. Legalex GS expone a todos los suscriptores y posibles clientes los términos y condiciones con respecto al uso de su servicio de emisión de Constancias de Conservación de Mensajes de Datos.

6. La declaración y las políticas de CCMD, así como toda la documentación pertinente es revisada y aprobada por la Secretaría de Economía, así como por la PSC de Legalex GS.
7. El Director Ejecutivo de Legalex GS, así como el Profesional Jurídico y el Profesional Informático son los encargados de asegurar que se implementen correctamente todas las políticas de CCMD descritas en los documentos.
8. En el Apéndice C se establece un calendario de revisión para mantener las políticas y la declaración de prácticas actualizadas.
9. Cualquier cambio que surja y que impacte en las funciones/servicios de Legalex GS, deberán de ser notificados con la debida antelación a la Secretaría de Economía para que sean revisados y los cambios estén disponibles de manera inmediata para suscriptores y posibles clientes.

Declaración de divulgación del PSC

El PSC divulgará a todos los suscriptores y partes que confían, las políticas y declaración de prácticas de Constancias de Conservación de Mensajes de Datos, así como el aviso de privacidad y los términos y condiciones relacionados con el uso de su servicio de emisión de Constancias de Conservación de Mensajes de Datos a través de su sito electrónico:

https://www.legalexgs.com

Así mismo los documentos que sean publicados en el sitio electrónico quedarán en carácter de públicos, y como tales no contendrán información que Legalex GS considere sensible.

Para cada Constancia de Conservación de Mensajes de Datos que sea proveído por la ACCMD de Legalex GS se especifica dentro de la presente declaración, y en las políticas la siguiente información:

1. La información de contacto de la PSC: Periférico Paseo de la República No. 2650, Piso 2 Interior 3-C Colonia Prados del Campestre, Morelia, Michoacán. C.P. 58297
2. Las políticas de Constancias de Conservación de Mensajes de Datos que se aplican de forma pública en su sitio web antes mencionado.
3. El algoritmo Hash con el que se representan los datos de las Constancias de Conservación de Mensajes de Datos. El cual corresponde al SHA-256 según las políticas de Constancias de Conservación de Mensajes de Datos.
4. El periodo de validez del certificado de CCMD de la ACCMD es de 10 años a partir de la expedición del certificado de Constancias de Conservación de Mensajes de Datos emitido por la Secretaría de Economía, para la ACCMD de Legalex GS.
5. Las limitaciones del servicio que se especifican en este documento en el apartado de limitaciones de la responsabilidad, así como en el contrato de prestación de servicios de CCMD firmado por el cliente/suscriptor que lo contrata.
6. Las obligaciones tanto del suscriptor como de la parte que confía se especifican en este documento en el apartado de obligaciones y

responsabilidades, cumpliendo con las Reglas Generales a las que deberán sujetarse los PSC en su **Regla 163** y conforme lo dicta el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280.

7. Para verificar la información y validación de las Constancias de Conservación de Mensajes de Datos, donde las partes que confían puede acceder a verificar el estado de la constancia, cumpliendo con el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280: https://www.legalexgs.com/Servicios/sellos/validarNOM.jsp.
8. El período de conservación de los registros y documentos que se expiden de la contratación del servicio de CCMD y los sucesos de la ACCMD por parte de los suscriptores, tendrá un tiempo de conservación de **10 años,** a partir de la firma del contrato.
9. El Profesional Jurídico será quien atienda cualquier reclamo que surja, y deberá de dar solución apegándose a la legislación nacional y los reglamentos de la Secretaría de Economía y en un tiempo no mayor a 30 días naturales.
10. Las limitaciones de la Constancia de Conservación de Mensajes de Datos se especifican en este documento en el apartado de obligaciones y responsabilidades.
11. La Secretaría de Economía realiza las auditorías pertinentes para evaluar a la PSC y que cumple con los requisitos identificados. La forma en que se realizan estas auditorías depende totalmente de la Secretaría de Economía.
12. En caso de presentarse alguna falla en el sistema de la ACCMD, esta deberá de atenderse por el Profesional Informático en un tiempo no mayor a 30 minutos y se notificará a los suscriptores y a la SE acerca de la falla según se especifica en el manual de plan de recuperación ante desastres.
13. El Procedimientos para reclamos y resolución de disputas se efectuará directamente con el Profesional Jurídico a través del siguiente correo electrónico privacidad@legalexgs.com

Gestión del ciclo de vida de las llaves

Generación de las Claves de la ACCMD

Legalex GS asegura que generará y usará todas las llaves criptográficas bajo las siguientes circunstancias:

1. La generación de las claves públicas y privadas para la Unidad de Constancias de Conservación de Mensajes de Datos se realizan bajo situaciones controladas y seguras. La generación estará a cargo del Profesional Informático.
2. Para la generación de las claves se utiliza un dispositivo criptográfico HSM con una certificación nivel 3 acorde al estándar FIPS 140-2, como se especifica en el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280. Cumpliendo así con la **Regla 140**, numeral II de las reglas generales a las que deberán sujetarse los PSC.
3. El algoritmo utilizado para la generación de las claves criptográficas de la ACCMD y la Unidad de Constancias de Conservación de Mensajes de Datos será RSA con SHA-256, empleando una longitud de clave de 4096 bits.

Dentro del proceso de generación de claves de la ACCMD, existen tres motivos principales por los cuales la ACCMD de Legalex GS solicitará la emisión de un nuevo certificado de CCMD a la entidad certificadora raíz:

1. Generación de certificado de CCMD por primera ocasión: se solicitará la emisión del certificado de CCMD que avale a Legalex GS como Prestador de Servicios de Certificación, una vez que sea acreditado por Secretaría de Economía, por primera ocasión. No existirán certificados emitidos ni revocados por la ACCMD en este punto.
    a. La generación del certificado para el servicio de CCMD es realizado dentro del security world. El proceso consta en que el Profesional Informático cree el ecosistema seguro dentro de una ceremonia de llaves dentro del HSM para la ACCMD, donde se seleccionará el número de administradores que existirán y si existirán controles remotos. Se asignan las claves para cada partición y rol y se procederá a la creación de las claves para la firma del servicio emisión de Constancias de Conservación de Mensajes de Datos.
2. Generación de certificado por renovación de vigencia: una vez que la ACCMD haya comenzado a operar y la vigencia del certificado emitido por Secretaría de Economía esté próximo a caducar (aproximadamente 2 años antes de la perdida de vigencia), se solicitará la emisión de un nuevo certificado que comenzará a operar de manera inmediata. La solicitud del nuevo certificado debe realizarse con un máximo de seis meses de anticipación, antes de la expiración del certificado de CCMD próximo a caducar y de acuerdo con las especificaciones de la legislación vigente en ese entonces.
3. Generación de certificado de Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) por revocación: se solicitará de manera inmediata la emisión de un nuevo certificado de ACCMD para la ACCMD que reemplace y anule el certificado anterior. Esta acción puede suscitarse debido a que las llaves de la ACCMD se encuentran comprometidas y se debe revocar inmediatamente el certificado de ACCMD ante la AC raíz Secretaría de Economía. La solicitud del nuevo certificado debe realizarse por el método que se considere más veloz y eficaz, avalado por Secretaría de Economía.

Protección de claves.

[Visualizar contenido en la versión privada]

Distribución de la clave pública de la ACCMD

La PSC se asegurará de que la integridad y la autenticidad de la ACCMD y cualquier parámetro asociado se mantienen durante su distribución a las partes que confían.

Renovación (nueva emisión) de las claves de la ACCMD

El tiempo de vida de los certificados de ACCMD serán específicamente de diez años. Ante esto, Legalex GS renovará las claves de sus ACCMD por lo menos dos años antes de que estas expiren.

Fin del ciclo de vida de las claves de la ACCMD

Una vez expirado el certificado, la llave privada puede ser generada con la misma clave y en el mismo security world siempre y cuando el certificado haya expirado o haya sido revocado por el reemplazo de un nuevo certificado, se pedirá la emisión o renovación del certificado de CCMD a Secretaría de Economía.

Gestión del ciclo de vida del módulo criptográfico usado para las Constancias de Conservación de Mensajes de Datos

[Visualizar contenido en la versión privada]

Sobre el servicio de Constancias de Conservación de Mensajes de Datos

La ACCMD de Legalex GS cumplirá con los estándares señalados en el RFC 3161 *Time-Stamp protocol (TSP)* y el RFC 3628 *Policy Requirements for Time-Stamping Authorities (TSAs)* para garantizar la calidad, el rendimiento y el funcionamiento del servicio de Constancias de Conservación de Mensajes de Datos.

Token o identificador de Constancias de Conservación de Mensajes de Datos

Las constancias generadas por la ACCMD de Legalex GS deben cumplir con las especificaciones técnicas del estándar RFC 3161 (IETF, 2018), así como el uso de una de las extensiones señaladas en el RFC 5280. Además, la ACCMD asegurará que los identificadores de la CCMD se emitan de forma segura e incluyan la hora correcta de una unidad de tiempo confiable.

Vigencia de la Constancia de Conservación de Mensajes de Datos

Legalex GS en concordancia con lo establecido en la NOM-151-SCFI-2016 en su apartado A.8.4.1 establece que la vigencia de las Constancias de Conservación de Mensajes de Datos emitidas por su ACCMD será de 10 años a partir de su emisión. Una vez cumplido este periodo el comerciante podrá decidir si requiere la extensión de dicho periodo según la naturaleza de la información y de acuerdo con los ordenamientos legales aplicables.

Gestión y operación del CCMD

Requerimientos para operar el servicio

Las personas físicas o morales que requieren los servicios proporcionados por la Autoridad de Constancias de Conservación de Mensajes de Datos y que aceptan explícita o implícitamente sus términos y condiciones establecidos en un contrato de prestación de servicios debe contar con los siguientes requerimientos:

1. Contratación del servicio de CCMD.

2. Una aplicación cliente compatible con el RFC 3161 Time-Stamp Protocol (TSP), así como el uso de una de las extensiones señaladas en el RFC 5280.
3. Acceso a internet mediante un navegador web compatible (Chrome, Firefox, safari, Microsoft Edge).
4. Equipo de cómputo para acceder al servicio, en caso de ser una conexión tipo cliente-cliente el proveedor que consuma nuestros servicios, tendrá la obligación de darle las indicaciones pertinentes a sus clientes finales.

Legalex GS a través del departamento de ventas o comercial, realiza presentaciones para ofrecer el servicio de CCMD y atiende las necesidades de los suscriptores que son los interesados en el servicio.

Así mismo, la PSC, se asegurará de la administración de los procedimientos aplicados y que estos correspondan a las buenas prácticas para la gestión y administración de seguridad en conjunto con el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad:

1. El PSC retendrá la responsabilidad de la prestación de servicios de CCMD dentro del alcance que marca la presente declaración de prácticas de CCMD y las políticas de CCMD.
2. La dirección o el Director Ejecutivo de Legalex GS deberá proporcionar y hacer cumplir en conjunto con el Profesional Informático y el Auxiliar de Apoyo Informático de Seguridad, las instrucciones y métodos que habrán de seguirse sobre la seguridad de la información y las buenas prácticas que han de seguirse, las cuales se encuentran en el documento titulado Políticas de seguridad de la información. La PSC deberá publicar a sus empleados estás políticas para que se encuentren enterados de los requerimientos que deben de seguirse.
3. Asegurarse de contar con la infraestructura de seguridad de la información necesaria y la mínima contemplada por la Secretaría de Economía en las Reglas generales que deberán de sujetarse los PSC en su capítulo IV "*De los elementos tecnológicos*".
4. Seguir los lineamientos marcados en el SGSI.
5. Los controles de seguridad y procedimientos operativos para las instalaciones donde se encuentre la ACCMD, marcados por el centro de datos de TRIARA, así mismo, mantener documentado, actualizado y asegurado toda aquella infraestructura que dependa del correcto funcionamiento de la provisión de Constancias de Conservación de Mensajes de Datos.
6. La PSC y la ACCMD se deberán de asegurar de que se mantenga la seguridad en la información, cuando la responsabilidad de las funciones de la ACCMD sea subcontratada u otra organización o entidad.

Clasificación y gestión de activos

[Visualizar contenido en la versión privada]

Solicitud de servicio

Los suscriptores del servicio de CCMD deberán de formalizar el contrato de servicio a través de los siguientes pasos:

1. Agendar una cita marcando al teléfono institucional, pedir una cotización del servicio y de estar de acuerdo pasar al siguiente paso.
2. Entregar toda la documentación que se pida al cliente / suscriptor. Como lo son datos generales: nombre completo, razón social, RFC, pagos, copias de la documentación.
3. Celebrar un contrato de prestación de servicios con Legalex GS donde acuerde el suscriptor estar de acuerdo con lo pactado en el contrato.
4. Firmar el contrato de prestación del servicio de Constancias de Conservación de Mensajes de Datos.
5. Guardar y cuidar las credenciales de acceso que se le den para comenzar el uso del servicio de CCMD.

Gestión y clasificación de los activos

[Visualizar contenido en la versión privada]

Seguridad del personal

[Visualizar contenido en la versión privada]

Sobre el control de seguridad del personal

[Visualizar contenido en la versión privada]

Proceso de Reclutamiento

[Visualizar contenido en la versión privada]

Seguridad física y ambiental

[Visualizar contenido en la versión privada]

Gestión de controles físicos

[Visualizar contenido en la versión privada]

Sobre el acceso físico

[Visualizar contenido en la versión privada]

Sobre la Destrucción de documentos
[Visualizar contenido en la versión privada]

Gestión de operaciones
[Visualizar contenido en la versión privada]

Gestión de acceso a los sistemas
[Visualizar contenido en la versión privada]

Mantenimiento e implementación de sistemas de confianza
[Visualizar contenido en la versión privada]

Compromiso de los servicios del PSC
En caso de que la clave privada de una ACCMD se vea comprometida, Legalex GS, procederá a notificar a la SE, revocar el certificado de la ACCMD y evitar la emisión de Constancias de Conservación de Mensajes de Datos firmados por dicho certificado, posteriormente se procederá a la solicitud de una nueva emisión de certificado, para reanudar las operaciones de la ACCMD lo más pronto posible.

Si existe evidencia o sospecha de pérdida de calibración de los relojes de la ACCMD que provee los tokens hacia la ACCMD no emitirá ninguna Constancia de Conservación de Mensajes de Datos hasta corroborar la recalibración y notificará a las partes interesadas que pudieran haber solicitado y recibido una constancia de conservación durante el percance.

Terminación y Sucesión de la ACCMD
En caso de la suspensión o disolución de la Autoridad de Constancias de Conservación de Mensajes de Datos, Legalex GS, tomará en cuenta las siguientes observaciones con el fin de minimizar el impacto en aquellos que se pudieran ver afectados por el cese de operaciones de la PSC:

1. Notificar a las autoridades o personal competente de la salida, baja o disolución de la PSC. Informar a todos los usuarios sin excepción alguna sobre los acuerdos a los que se han llegado, aviso y procedimientos para los usuarios.
2. Los usuarios de la ACCMD se darán de baja y serán bloqueados de la plataforma por el administrador o el Auxiliar de Apoyo Informático de Seguridad de Legalex GS.
3. Toda la documentación personal o propia de todo el personal que laboró en las oficinas será debidamente conservada y resguardada para auditorías y procesos administrativos de Legalex GS, así mismo se considera que se conserve para la reactivación en caso de haber una baja o suspensión temporal de las actividades de la PSC.

4. La PSC que continúe con las operaciones de la ACCMD Legalex GS (seleccionado o determinado por la Secretaría de Economía), debe de cumplir en la proximidad posible, con las responsabilidades y obligaciones que se tenían en un principio, para que el usuario suscriptor recienta en lo menor posible el cambio.
5. En caso de no encontrar una PSC alterna que pueda brindar el servicio a los clientes de Legalex GS, la Secretaría de Economía determinará de acuerdo con lo dispuesto en la normatividad aplicable lo procedente.
6. La ACCMD de Legalex GS, procurará en lo posible no tener interrupciones en su servicio y provocar malestar a los suscriptores, así como a los terceros de confianza, tratando de asegurar en lo posible la continuidad y mantenimiento de la información y sus servicios.
7. Secretaría de Economía determinará cual PSC será el encargado de seguir ofreciendo el servicio de emisión a los suscriptores, o en su defecto SE ofrecerá el servicio.
8. La PSC procurará en lo posible no tener interrupciones en su servicio y provocar malestar a los suscriptores, así como a los terceros de confianza, tratando de asegurar en lo posible la continuidad y mantenimiento de la información y sus servicios.

Antes de que la ACCMD de Legalex GS finalice sus servicios de CCMD de ser el caso, realizará las siguientes actividades:

1. Pondrá a disposición de sus suscriptores y terceros de confianza la información sobre su terminación.
2. La PSC dará por terminada la autorización de todos los subcontratistas para actuar en nombre de la PSC en el desempeño de cualquier función relacionada con el servicio de emisión Constancias de Conservación de Mensajes de Datos.
3. La PSC transferirá sus obligaciones a una parte confiable como otro PSC o a la Secretaría de Economía, así como su mantenimiento de los registros de eventos y archivos de auditoría necesarios para demostrar el correcto funcionamiento de la ACCMD por un periodo razonable.
4. La PSC mantendrá o transferirá a una parte confiable (otra PSC con ACCMD o a la Secretaría de Economía) su obligación de poner a disposición su clave pública o su certificado de CCMD a partes confiables por un tiempo razonable.
5. Las claves privadas de la ACCMD, incluidas las copias de seguridad, se destruirán de una manera tal que las claves privadas no puedan ser recuperadas.
6. La PSC deberá tener un acuerdo para cubrir los costos cuando se encuentre en un estado de quiebra, pudiendo cubrirse con un seguro como se establece en las reglas generales a las que deberán sujetarse los PSC en su regla 84.
7. La PSC deberá indicar o notificar a las entidades correspondientes de su estado, mediante un correo electrónico marcado como importante o urgente, y en caso de emergencia, la PSC deberá de reportarlo vía telefónica a la SE y enviar vía correo postal el reporte correspondiente por escrito.

Cumplimiento de requerimientos legales

Legalex GS como Autoridad de Constancias de Conservación de Mensajes de Datos, actúa en conformidad con el código de comercio, título tercero "Del comercio electrónico" y cumple con lo estipulado en las reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación, establecido por la Secretaría de Economía, además, la ACCMD de Legalex GS se encuentra regulada por la Secretaría de Economía de los Estados Unidos Mexicanos y sigue las directrices técnicas establecidas por los estándares de organismos calificadores internacionales como ETSI, IETF y NIST.

Legalex GS, se compromete a proteger la información personal de sus suscriptores, manteniendo la confidencialidad y la integridad de los datos en cumplimiento a lo dispuesto por la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, tal y como se explica en el aviso de privacidad disponible en:

https://www.legalexgs.com/avisoprivacidad.pdf

Registro de información concerniente a las operaciones del servicio de emisión de Constancias de Conservación de Mensajes de Datos

Legalex GS, mantiene registros de las operaciones relacionadas con la solicitud, contratos, servicio y otros aspectos relacionados con la provisión de Constancias de Conservación de Mensajes de Datos.

Obligaciones y responsabilidades

Obligaciones

Obligaciones del PSC

Legalex GS, como Prestador de Servicios de Certificación, se asegurará de que todos los procedimientos detallados en la presente Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos se lleven a cabo:

1. Proporcionar el servicio de emisión de Constancias de Conservación de Mensajes de Datos de acuerdo con la presente declaración de práctica y su Política de Constancias de Conservación de Mensajes de Datos.
2. Usar, establecer y crear sistemas o plataformas que sean lo suficientemente seguras 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 las Constancias de Conservación de Mensajes de Datos emitidos o proveídos determinarán la fecha y la hora con la precisión establecida.

5. 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.
6. 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.
7. Realizar una revisión anual del presente documento y en su caso realizar las actualizaciones necesarias con la aprobación requerida.
8. 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.
9. Poner a disposición de los usuarios la Política de Constancias de Conservación de Mensajes de Datos privada, así como la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos pública en el sitio https://www.legalexgs.com.
10. Atender las inconformidades de los suscriptores 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 estará prestando.
11. 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.
12. Emitir CCMD conforme a la presente declaración de prácticas, las políticas de Constancias de Conservación de Mensajes de Datos y con la información que el suscriptor proporcionó en el momento que se requirió para la elaboración del contrato de servicios prestados por la PSC de Legalex GS.
13. La conservación por medios electrónicos de información y documentos que se relacionen con las Constancias de Conservación de Mensajes de Datos emitidos, así como los contratos de servicios durante al menos el lapso de 10 años desde su expedición, serán responsabilidad del Profesional Informático.
14. Los datos que se transmiten entre los sistemas o plataformas (toda información delicada) son usados y enviados sobre una conexión segura (VPN).
15. La PSC, así como la persona encargada de recabar la firma del contrato de servicios, tiene la obligación de dar a elegir al suscriptor o cliente, sí desea obtener algún otro servicio o no, estos no deben de ser obligatorios.
16. Brindar y prestar los servicios relacionados con la emisión de Constancias de Conservación de Mensajes de Datos.
17. La contratación específica y del perfil adecuado del personal que se encargará de asegurar la calidad del servicio.
18. Declaramos que queda estrictamente prohibido la reventa y copias no autorizadas del servicio de emisión de Constancias de Conservación de Mensajes de Datos de Legalex GS por un tercero.

Obligaciones de los Suscriptores

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:

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 emitidos por la ACCMD.
7. En caso de Personas Morales, sí el representante o apoderado legal son personas o entidades separadas, el que se suscriba o quede como titular del servicio, deberá informar a la persona Moral sobre las obligaciones a las que estará regido.
8. El suscriptor deberá dar información precisa y completa cuando se esté elaborando su contrato para la prestación de servicios.
9. Se tendrá el cuidado suficiente sobre los archivos provenientes de la Constancia de Conservación de Mensajes de Datos para evitar el mal uso de un documento ya firmado con su constancia respectiva.
10. Notificar a Legalex GS sin ningún retraso razonable, si se produce algún error o inexactitud en el servicio brindado, para que este sea resuelto lo más pronto posible.
11. Toda la información que el suscriptor dé debe ser verídica, ya que, si esta no coincide, el suscriptor no podrá solicitar los servicios de la PSC y podrá quedar expuesto a no volver a ser candidato de la prestación de cualquier servicio que Legalex GS le pueda brindar.
12. Tener a disposición el instrumento en el cual se guardará cualquier documento que emerja de la sesión de la prestación del servicio que solicite. Este debe tener suficiente espacio para los archivos, y asegurarse que no cuente con virus o archivos maliciosos.
13. Cumplir con lo pactado en los acuerdos y declaraciones que firmó con Legalex GS.
14. Utilizar de forma correcta el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

15. La reventa, copias y servicios no autorizadas de las Constancias de Conservación de Mensajes de Datos de Legalex GS por un tercero, queda prohibido y la PSC no se responsabilizará por este acto.

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 atendrán a los términos y condiciones de la ACCMD las cuales estipulan:

1. Verificar que el token recibido por parte del servicio de emisión 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 al servicio de emisión de Constancias de Conservación de Mensajes de Datos y/o a las constancias emitidas o proveídos.

Responsabilidades

Responsabilidades de la PSC.

Las responsabilidades principales que tiene Legalex GS como una ACCMD recaen en las siguientes:

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 válidos 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.
5. Cumplir con las revisiones y auditorias, así como acatar las recomendaciones que presenten los auditores para mejorar el servicio de la empresa.

6. Asegurar a los suscriptores, partes que confían y empleados, el correcto resguardo de la información privada, así como de las actividades de cada participante individual.
7. Las Constancias de Conservación de Mensajes de Datos emitidos por la ACCMD de Legalex GS, deben usarse únicamente en los casos establecidos en la declaración de prácticas de Constancias de Conservación de Mensajes de Datos en su apartado de aplicabilidad.
8. Estas responsabilidades no afectan una implicación directa en el cobro del servicio de emisión de Constancias de Conservación de Mensajes de Datos.
9. El detalle de todas las Responsabilidades de la PSC se integran en el contrato de servicios.
10. Negar o limitar cualquier responsabilidad a menos que se estipule lo contrario por la ley aplicable.

Responsabilidad de los suscriptores

Los suscriptores que hagan uso de las Constancias de Conservación de Mensajes de Datos deben acatar las siguientes responsabilidades:

1. Resguardar los archivos que se dan como efecto de cada CCMD, administrar sus propias copias de seguridad de los archivos que se emiten y los archivos provenientes del servicio.
2. Resguardar las claves empleadas para tener acceso al servicio de CCMD.
3. Mantener un uso correcto de sus credenciales para el servicio de CCMD, 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.
4. 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 se tomarán como verdaderas y cualquier dato falso podría ser causa de una penalización severa según la ley aplicable.
5. Asegurarse que su constancia solo sea usada para fines y propósitos comerciales ya autorizados, como son, asuntos del orden comercial conforme al Código de comercio en el artículo 101 numeral IV.
6. Cuidar el uso que se le dé al dispositivo o medio electrónico donde guarde sus credenciales o claves para el acceso de CCMD, así como otros documentos o archivos expedidos por el personal que le entregue el contrato de prestación del servicio de CCMD.

Limitaciones de la Responsabilidad

En este apartado se hablará sobre las limitaciones que se tienen en las responsabilidades expresadas en el documento, es decir, cuando se descarta la responsabilidad por factores principales como los son:

1. Daños y perjuicios.
2. Imprevistos involuntarios.
3. Accidentes directos o indirectos.

Descarto de responsabilidades

Mediante la *Declaración de Prácticas de Constancias de Conservación de Mensajes de Datos, se obtiene que Legalex GS.* no tendrá ni asumirá ninguna responsabilidad o compromiso cuando ocurra alguna de las siguientes situaciones:

1. El uso inadecuado o no autorizado de una Constancia de Conservación de Mensajes de Datos solicitados por algún suscriptor o cliente.
2. Constancias de Conservación de Mensajes de Datos emitidos o proveídos por terceras personas que tengan acceso a las credenciales de algún suscriptor.
3. Constancias de Conservación de Mensajes de Datos emitidos o proveídos con información fraudulenta o falsa, sin importar que el cliente o suscriptor del servicio lo tenga en su resguardo.
4. Constancias de Conservación de Mensajes de Datos emitidos sin el consentimiento de las personas involucradas, a la fuerza o sobre presión.
5. Que ocurra un siniestro de guerra, hostilidades militares o policiacas, o incluso la insubordinación que afecte directamente al PSC o al cliente/suscriptor del servicio, ambos quedarán deslindados de responsabilidades.
6. Que ocurra una legislación o acción gubernamental, prohibición, boicot, embargo, perturbaciones civiles, explosión, restricción comercial, legislaciones incongruentes, que decline alguna de las dos partes o que afecte directamente a la PSC, ACCMD o al cliente/suscriptor, ambos quedarán deslindados de responsabilidades.

Restricciones de uso de las Constancias de Conservación de Mensajes de Datos

Las Constancias de Conservación de Mensajes de Datos emitidos por la ACCMD de la PSC Legalex GS, pueden utilizarse únicamente en los términos que establece el código de comercio (artículo 101 numeral IV), en operaciones referentes a actos mercantiles, leyes aplicables, circulares y demás disposiciones que permitan su uso, sin perjuicio de su uso en actos de cualquier otra naturaleza en procesos en los que se incorpora una Constancias de Conservación de Mensajes de Datos.

El uso de las Constancias de Conservación de Mensajes de Datos queda limitado por sus políticas de uso y su aplicabilidad como se marcan en las Políticas de Constancias de Conservación de Mensajes de Datos en el tema *Identificación* y *Comunidad de usuarios y aplicabilidad*. La cual marca la siguiente información proveniente del identificador de objetos de las políticas X.208 del RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280:

Responsabilidades Económicas

Las responsabilidades económicas a las que la ACCMD se sujeta se determinan en dos partes:

1. Las responsabilidades económicas a las que la ACCMD de Legalex GS se visualizan específicamente con las indemnizaciones que debe realizar la PSC hacia la AC Raíz (Secretaría de Economía) o los suscriptores cuando se presente una responsabilidad.
2. Indemnización por parte de los Suscriptores, este punto será efectivo cuando los suscriptores caigan en las siguientes situaciones:
    a. Errores en la protección de la clave de acceso al titular del servicio de emisión de Constancias de Conservación de Mensajes de Datos
    b. Que el suscriptor utilice información falsificada o de mala exhibición durante la toma de datos y dentro de la solicitud del servicio.
    c. Que un suscriptor dañe a terceras personas con el uso del servicio.
    d. Negligencia en la revelación de datos o hechos importantes en la solicitud del CCMD, que fueron concebidos con dolo, con intensión de engañar a una persona, incluido el Director Ejecutivo o algún asesor de ventas.

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.

Políticas de Constancias de Conservación de Mensajes de Datos

Identificación

El identificador de objeto (X.208) utiliza la notación ASN.1 de la política de las Constancias de Conservación de Mensajes de Datos. El cual está basado en una estructura en árbol para las asignaciones realizadas por una estructura jerárquica de Autoridades de registro, denominada árbol OID internacional, la cual esta especificada en la ISO/IEC 9834-1:2012 (International Organization Standars).

Comunidad de usuarios y aplicabilidad

Está política tiene como objetivo cumplir los requisitos para la firma electrónica, calificada para ser usada con la Constancia de Conservación de Mensajes de Datos o en su defecto los certificados que se utilizarán para el proceso de emisión de Constancias de Conservación de Mensajes de Datos. La estructura utilizada en el proceso de emisión de las Constancias de Conservación de Mensajes de Datos se define en el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280. 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 deberán sujetarse los Prestadores de Servicios de Certificación.

Conformidad

Todos los servicios de emisión de Constancias de Conservación de Mensajes de Datos que utilicen a la Autoridad de Constancias de Conservación de Mensajes de Datos llevarán un identificador, la causa es que la ACCMD utiliza y utilizará el identificador de las políticas de Constancias de Conservación de Mensajes de Datos en el token o identificador de las Constancias de Conservación de Mensajes de Datos, como se explica en el tema "*Identificación*" de este documento.

Legalex GS reclamará la conformidad con el presente documento aplicado en las políticas de Constancias de Conservación de Mensajes de Datos, identificando la constancia que se emiten bajo la ACCMD, cumpliendo con los siguientes requerimientos: 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 identificada dentro de las constancias que se emita bajo la ACCMD de Legalex GS que pone a disposición de los suscriptores 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 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 externo no debe de tener una relación jerárquica con el departamento que opera la ACCMD. Las auditorias deberán realizarse por un auditor independiente y competente, como se establece en la *RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280.*
3. La ACCMD demostrará que cumple con sus obligaciones tal y como se define en el título *Obligaciones de la ACCMD* de este mismo documento.
4. La PSC implementará los controles que cumplan con los requisitos de la Declaración de prácticas de Constancias de Conservación de Mensajes de Datos.
5. Cuando exista la evaluación de conformidad con las políticas de Constancias de Conservación de Mensajes de Datos y los procesos auditados por parte de la ACCMD; los resultados de la evaluación se pondrán a disposición de los suscriptores y las partes que confían que lo soliciten, así como a la Secretaría de Economía.
6. Legalex GS puede emitir certificados de constancias 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".
7. De no cumplir con lo establecido en la presente Declaración de Prácticas 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 deberán sujetarse los PSC, emitido por la Secretaría de Economía respectivamente, Legalex GS dejará de emitir Constancias de Conservación de Mensajes de Datos y proveer sus servicios, hasta que haya demostrado lo

contrario; Legalex GS tomará las medidas necesarias para remediar la "no conformidad" dentro de un periodo razonable.

El cumplimiento respecto a la ACCMD se verificará regularmente y cada vez que se realice un cambio importante en sus operaciones.

Aplicabilidad

Las Constancias de Conservación de Mensajes de Datos que proporciona Legalex GS solo serán emitidos a usuarios que hayan celebrado un contrato de prestación de servicios con Legalex GS sobre el servicio de CCMD, los cuales están diseñados con apego a lo establecido en el código de comercio y leyes aplicables que permitan dar uso principalmente en contextos jurídicos y serán emitidos para las finalidades que se describen en el tema de *Servicios de* Constancias de Conservación de Mensajes de Datos.

La declaración de prácticas de CCMD va en cumplimiento con las reglas generales a las que deberán sujetarse los PSC en su regla 163, que establece la Secretaría de Economía para ofrecer el servicio de emisión de Constancias de Conservación de Mensajes de Datos.

La Constancia de Conservación de Mensajes de Datos que expedirá la ACCMD Legalex GS se generarán de acuerdo con lo establecido por la Secretaría de Economía, el estándar internacional "Internet X.509 Public Key Infrestructure Time Stamp" y el RFC 3161, así como el uso de una de las extensiones señaladas en el RFC 5280.

Organización

Legalex GS se acreditará como PSC por la Secretaría de Economía de los Estados Unidos Mexicanos y se encontrará habilitada como una Autoridad de Constancias de Conservación de Mensajes de Datos (ACCMD) y como tal cumplirá con las siguientes clausulas:

1. Las políticas y procedimientos bajo los cuales opera la ACCMD no son discriminatorias.
2. Legalex GS, pondrá sus servicios como ACCMD a todos sus suscriptores que cuenten con un contrato de prestación de servicios con la PSC Legalex GS, acepten las obligaciones descritas en este documento y cumplan con las prácticas y políticas de la ACCMD.
3. Legalex GS, cumple con las normas legales vigentes en los Estados Unidos Mexicanos, tal como se expresa en la sección "Cumplimiento de requerimientos legales" de este documento.
4. Legalex GS, garantiza que sus sistemas son seguros y confiables, ya que para lograr la acreditación por parte de la SE, los sistemas fueron concebidos y son operados bajo los más altos estándares internacionales establecidos por instituciones como ISO, ETSI, IETF y NIST.

5. Todos los procesos, planes de contingencia, prácticas y políticas de Legalex GS, se encuentran debidamente documentados y son revisados y actualizados periódicamente.
6. Todo el personal de Legalex GS está debidamente calificado y cumple con los requisitos expresados en las reglas generales a las que deberán sujetarse los prestadores de servicios de certificación publicadas por la SE en 2018.
7. Legalex GS, tiene disposiciones adecuadas para cubrir responsabilidades derivadas de sus operaciones y/o actividades, las cuales, se encuentran detalladas en este documento.
8. Legalex GS tiene y demostró ante la SE la estabilidad financiera y los recursos necesarios para operar como una ACCMD; sin embargo, en caso del cese de actividades de la ACCMD, Legalex GS cuenta con procedimientos para minimizar el impacto en aquellos que se pudieran ver afectados. Estos procedimientos se explican en la sección "Terminación de la Autoridad de Constancias de Conservación de Mensajes de Datos".

Consideraciones de seguridad

Al verificar los tokens o identificadores de Constancias de Conservación de Mensajes de Datos, es necesario, que el cliente que verifica la disponibilidad del CCMD, se asegure de que el certificado de la ACCMD sea confiable y no se encuentre revocado. Esto significa que la confiabilidad depende de la seguridad de la ACCMD que ha emitido el certificado para la PSC de Legalex GS, en este caso el certificado de CCMD firmado por la Secretaría de Economía será de un periodo de 7 años.

Todas aquellas entidades que confíen en las Constancias de Conservación de Mensajes de Datos emitidas por Legalex GS, deben de asegurarse de que el certificado de firma de la ACCMD se encuentre vigente, a través de los servicios de consulta de la comprobación del estado de los certificados, entre los cuales se incluye:

1. Características de operación del servicio en cuestión a la comprobación del estado del certificado.
2. La disponibilidad del o los servicios de consulta.
3. Para la verificación del estado y servicio de consulta de cada CCMD emitido o proveído por la ACCMD, consultar el sitio https://www.legalexgs.com/Servicios/sellos/validarNOM.jsp.

Todos los servicios de consulta y validación de los CCMD estarán disponibles las 24 horas del día, durante todo el año.

Auditorías

[Visualizar contenido en la versión privada]

Anexos

Apéndice A

Acrónimos

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

Acrónimo	Significado
ANSI	Instituto Nacional Estadounidense de Estándares. (ANSI, 2017)
ACCMD	Autoridad de Constancias de Conservación de Mensajes de Datos.
CCMD	Constancia de Conservación de Mensajes de Datos.
CENAM	Centro Nacional de Metrología.
ETSI	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)
FIPS 140	Acrónimo de *Federal Information Processing Standard*, el cual contiene una publicación (140) que maneja los estándares de seguridad de ordenadores para la acreditación de módulos criptográficos. (Seagate, 2012)
FIPS 140-2	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 Standars and Technology, 2001)
HSM	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)
ICREA	Acrónimo de International Computer Room Expert Association. (International Organization for Standardization - ISO, 2017)
IEC	Siglas de *International Electrotechnical Commission*, es una organización de normalización en los campos eléctricos, electrónico y tecnologías relacionadas. (IEC - International Electrotechnical Commision, 2017)
IETF	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)
ISO	Siglas de *International Organization for Standardization*, la Organización internacional de estandarización es un sistema que normaliza de forma internacional productos de áreas diversas. (International Organization for Standardization - ISO, 2017)

ITU-T	Siglas del Sector de Normalización de las Telecomunicaciones de la Unión de telecomunicaciones. (ITU, 2017)
NIST	Acrónimo de Nacional Institute of Standards and Technology. (NIST, National Institute of Standars and Technology, 2001)
PSC	Prestadora de servicios de certificación, hace referencia a la persona o institución pública que presta los servicios relacionados con la Firma electrónica y que expide los certificados. (Secretaria de Economía, 2007)
RFC	Acrónimo de *Request for comments*, que no es más que una serie de publicaciones que hacen a través de internet mediante la IETF (Engineering Task Force). (IETF, 2015)
RFC 5208	Protocolo que reglamenta los estándares criptográficos como los de la clave pública y la información de la clave privada sobre la información de sintaxis. (IETF, 2008)
RSA	Es un algoritmo asimétrico cifrado de bloques que utiliza una clave pública y una privada que se representan mediante números que se basan en el producto de dos números primos grandes elegidos al azar. (Seguridad Informática, 2007)
SE o S.E.	Secretaría de Economía.
SHA2-256	SHA2 es un Hash (función criptográfica que se crea mediante un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una serie de caracteres con longitud fija) de un certificado SSL siendo un algoritmo criptográfico desarrollado por el NIST y la NSA. (DigiCert, 2013)
USB	Universal serial bus, medio de almacenamiento digital o tipo de puerto de conexión universal para transferencia de datos. (Pérez Porto & Gardey, 2008)
X.500	Conjunto de estándares sobre servicios de un directorio, como pudieran ser las bases de datos de direcciones electrónicas. (IETF, 2015)
X.509	Estándar de criptografía para infraestructuras de claves públicas, este estándar especifica los formatos estándares para certificados de claves públicas y los algoritmos de validación de la ruta de certificación. (Via Firma developers, 2017)

Tabla 4Acrónimos

Definiciones

El siguiente apéndice contiene las definiciones para la terminología de seguridad utilizada en este manual, el cual está basado en los términos que establece el NIST 800-30 R1.

Definición	Significado
Bouncy Castle	Colección de APIs utilizadas en criptografía. (Legion of the Bouncy Castle Inc., 2013)
Certificado	Mensaje de dato o registro que confirme el vínculo entre un firmante y un dato digital que lo representa como su firma autógrafa. (Viafirma, 2017)
Firma electrónica	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)
Firmante	Es considerada como la persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa (en caso de ser Moral), de acuerdo con el artículo 89 del código de comercio. (Cámara de Diputados del H. Congreso de la unión, Secretaría de Economía, 2017)
Llave privada	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)
Llave pública	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)
Mensaje de datos	Hace referencia a la información generada, recibida, enviada, archivada o administrada por medios electrónicos, ópticos, digitales o tecnológicos, presentes en el artículo 89 del Código de Comercio. (Cámara de Diputados del H. Congreso de la unión, Secretaría de Economía, 2017)
Middleware	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)
Parte que confía	Hace referencia a la persona que siendo o no el Destinatario, actúa sobre la base de un certificado o una firma electrónica. (Secretaría de Economía, 2008)
Rack	Soporte metálico que guarda o aloja equipamiento electrónico, comúnmente equipo de infraestructura de redes. (Pérez Porto & Gardey, 2008)

SITE	Lugar donde se concentra el centro de procesamiento de datos, como lo es la infraestructura de red. (RAE - Real Academia Española, 2017)
Suscriptor	Se entiende por suscriptor, toda aquella persona física o moral que es titular de un certificado digital, donde voluntariamente confía y hace uso de su certificado digital emitido por la Autoridad Certificadora. (Secretaría de Gobernación SEGOB, 2012)
Token	Dentro del ambiente de la firma, son conocidos como OTP Tokens (one-time-password, contraseña de un solo uso), donde se general claves que solo pueden ser utilizadas una vez y para un fin único. En este caso la revocación de un certificado o la introducción de algún usuario a una plataforma específica. (Porras, 2015)
Web Service	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 Glosario de definiciones

Apéndice B

[Visualizar contenido en la versión privada]