



LEGALEX GS[®]

Políticas de Sellos digitales de tiempo

Para el Sellado digital de tiempo

... world ready. The strategy will be...
... with the right level of marketing...
... to see you gain value by...
... marketing approaches to...
(1) It is a promise to share an organization's...
(2) Marketing strategy's goal is to...
(3) The objectives will be based on how you...
(4) Marketing strategy helps to...
(5) Putting your strategy into action...
... how you're going to work with your...
... customer buying cycles will help you...
... let how your sales are followed up...
... if a program should be measured...
(6) Brand messages are delivered and...
... brand communication and distribution...

Signature 1

VERSIÓN PÚBLICA

OID: 2.16.484.101.10.316.100.6.1.3.11

PSC LEGALEX GS SA de CV
Morelia, Michoacán 2018

Esto es una **versión pública** y **no contiene** todo el material completo de las Políticas de Sellos digitales de tiempo 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 SELLOS DIGITALES DE TIEMPO VERSIÓN PÚBLICA

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

OID: 2.16.484.101.10.316.100.6.1.3.11

LEGALEX GS S.A. DE C.V.

RFC LGS160502EA8

Derechos reservados.

Fecha de revisión: _____.

LEGALEX GS S.A. DE C.V.

Copyright © 2016

Periférico paseo de la Republica 2650,

Número interior 3-C, piso 2.

Prados del Campestre, C.P. 58297.

Morelia, Michoacán, México.

Teléfono: (01 443) 690 68 51 ó 52

E-mail: 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 Sellos digitales de tiempo.....	6
Actores y entidades participantes en la infraestructura de la emisión de sellos digitales de tiempo.....	7
Conceptos generales.....	7
Servicios del Emisión de Sello digital de tiempo.....	7
Autoridad de Sellado de Tiempo (TSA).....	8
Suscriptores.....	8
Política de Sello digital de tiempo.....	9
Identificación.....	9
Comunidad de usuarios y aplicabilidad.....	9
Conformidad.....	10
Ciclo de vida de las llaves.....	10
Estampado de tiempo.....	11
Token o identificador de Sello Digital de Tiempo.....	11
Algoritmo de encriptación de datos.....	11
Sincronización del reloj con la hora UTC.....	12
Obligaciones y responsabilidades.....	12
Obligaciones.....	12
Obligaciones del PSC.....	12
Obligaciones de los Suscriptores.....	13
Obligaciones de la parte que confía.....	13
Responsabilidades del PSC.....	14
Responsabilidades de los suscriptores.....	14
Descarto de responsabilidades.....	15
Limitaciones del servicio.....	15
Responsabilidades Económicas.....	15
Términos y condiciones.....	15
Anexos.....	16

Apéndice A.....	16
Acrónimos.....	16
Glosario	17
Apéndice B.....	18
Bibliografía.....	18

Tabla de cuadros y esquemas

TABLA 1 IDENTIFICACIÓN DEL DOCUMENTO	4
TABLA 2 RESPONSABLES DE REVISIÓN	4
TABLA 3 AUTORIZACIÓN.....	5
TABLA 4 ACRÓNIMOS.....	16
TABLA 5 DEFINICIONES.....	17

Identificación del documento

En esta sección se identifican los datos principales del documento:

Nombre	Políticas de Sellos Digitales de Tiempo
Versión	1
Autor	Legalex GS.
Estado	Finalizado.
Fecha de emisión	17 de mayo del 2019
Fecha de elaboración	19 de octubre del 2018
Fecha de actualización	22 de mayo del 2019

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.

Cargo	Responsable	Firma
Líder y director de Proyecto	Joaquín Alcántar Hernández.	
Profesional informático	Ignacio Mota Cruz	
Auxiliar de apoyo informático de seguridad	Marco Antonio Pacheco Alvarez	
Profesional Jurídico	Antonio Mendoza Laurel	

Tabla 2 responsables de revisión

Autorización

La persona encargada de autorizar y dar el visto bueno del documento es el Profesional Informático de Legalex GS.

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

Tabla 3 Autorización

Introducción

El presente documento contiene las *Políticas de Sellos Digitales de Tiempo*, de la Autoridad de Sellado de Tiempo (TSA) Legalex GS S.A. de C.V., donde se establecen las reglas que se llevan a cabo para la prestación de servicios fiables de sellos digitales de tiempo.

Los servicios de Sello Digitales de Tiempo ofrecidos por Legalex GS están regidos por las *“Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación”*, Regla 116, 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 3628 *“Policy Requirements for time-Stamping Authorities (TSAs)”* o en sus capítulos 4, 5 y 6.

Alcance

Este documento detalla los requerimientos que debe cumplir el servicio de la Autoridad de Sellado de Tiempo (TSA) de Legalex GS con respecto a la provisión y administración de sellos digitales de tiempo.

Enfoque

El enfoque de una política de sello digital de tiempo es significativamente diferente de una declaración de práctica de TSA. Una política de sello digital de tiempo se define independientemente de los detalles específicos del entorno operativo específico de un TSA, mientras que una declaración de práctica de TSA se adapta a la estructura organizativa, los procedimientos operativos, las instalaciones y el entorno informático de una TSA. El usuario de los servicios de sellos digitales de tiempo puede definir una política de marca de tiempo, mientras que la declaración de práctica de TSA siempre la define el proveedor.

Administración de cambios de las Políticas de Sellos digitales de tiempo

Todas aquellas modificaciones que surtan efecto dentro de las *Políticas de sellos digitales de tiempo* y la *Declaración de prácticas de sellos digitales de tiempo* 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 nueva 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 sellos digitales de tiempo

Existen actores y entidades que participan dentro de la infraestructura de emisión de sellos digitales de tiempo, cada uno de ellos desempeñan distintos roles durante el proceso de emisión de un sello digital de tiempo, los actores implicados son:

1. Una Autoridad Certificadora Raíz, En este caso la Secretaría de Economía (SE).
2. Una Prestadora de Servicios de Certificación, siendo está Legalex GS.
 - o Una Autoridad de Sellado digital de tiempo (TSA), encargada del sistema de emisión o provisión y otros procesos relacionados con el sello digital de tiempo.
3. Los suscriptores o entidades finales, las personas u organizaciones que solicitarán el servicio de emisión de sello digital de tiempo, que podrían también llamarse "solicitantes".
4. Centro Nacional de Metrología (CENAM) es el organismo público federal de referencia en materia de mediciones que tiene como función, entre otras, sincronizar el tiempo UTC en base a relojes atómicos.
5. Parte que confía, son aquellos que expresan su "fe" en la Autoridad de Sellado Digital de Tiempo al creer que sus servicios son lo suficiente confiables. Por lo general, estos suelen ser también suscriptores.

Conceptos generales

Servicios del Emisión de Sello digital de tiempo

Los sellos digitales de tiempo de Legalex GS están diseñados para probar que un dato existía antes de la fecha y hora de emisión del citado sello, 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 durante la emisión de certificados digitales (para firma electrónica avanzada) el registro de la operación.
2. Proveer el servicio de emisión de sellos digitales de tiempo para las firmas electrónicas, especialmente a las avanzadas.
3. Preservar la hora y fecha de recepción de una firma electrónica en archivos de larga duración.
4. Proveer el mecanismo para saber el momento en que se generó una o varias constancias de Conservación de Mensaje de Datos.

5. Proveer la fecha y hora para la acreditación el momento en que se realiza un acto jurídico y comercial por medios electrónicos.

Los servicios que proveerá el PSC mediante la contratación de los sellos digitales de tiempo se dividen en los siguientes:

1. La provisión o emisión de sellos digitales de tiempo, este componente del servicio genera un token o identificador de transacción del sello digital de tiempo.
2. Validación del sello digital de tiempo, este componente es público y se encarga de validar que el sello digital de tiempo en un archivo es válido.

Autoridad de Sellado de Tiempo (TSA)

La autoridad emitirá tokens de sello de tiempo o identificadores de confianza por transacción que el suscriptor o cliente final del servicio de emisión de sellos digitales de tiempo realice. TSA tiene la responsabilidad de llevar a cabo correctamente el servicio de emisión de sellos digitales de tiempo que se nombran en el tema *Servicios de emisión de Sellos digitales de tiempo* dentro de este documento.

La TSA es responsable de la operación de la unidad de sellado de tiempo (TSU), es decir, las transacciones que se crean y firman en nombre del TSA y el suscriptor o receptor de la transacción. Como se piden en las *Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación, en el capítulo IV, De los elementos tecnológicos*, en la regla 123.

El PSC cuenta con una unidad de sellado de tiempo principal y su redundante. Cada unidad tiene una clave diferente. El tiempo seguro que provee el CENAM se sincroniza con el servidor de tiempo o reloj dentro de la TSU.

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 TSA que lo emite:

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 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 este 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 Sello digital de tiempo

Los procesos que usará Legalex GS y su Autoridad de Sellado Digital de Tiempo para crear marcas de tiempo y mantener la precisión del reloj o la hora sincronizada por el laboratorio nacional de referencia en materia de mediciones conocido por sus siglas como CENAM.

Identificación

El identificador de objeto (X.208) utilizando en la notación ASN.1 de las políticas de sellos de tiempo es:

```
itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023)  
policy-identifiers(1) baseline-ts-policy (1)
```

En la declaración de prácticas de Sellos Digitales de Tiempo versión pública que está disponible para los suscriptores y las partes que confían se incluye el identificador de las políticas de sello digital de tiempo que indican nuestra conformidad, una vez autorizada la acreditación de PSC por Secretaría de Economía.

Comunidad de usuarios y aplicabilidad

Esta política tiene como objetivo cumplir los requisitos para la firma electrónica calificada para ser usada con el sello digital de tiempo o en su defecto los certificados que se utilizarán para el servicio de emisión de sello digital de tiempo. El tipo de certificado utilizado para el servicio de emisión de sellos digitales de tiempo 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 sellos digitales de tiempo como lo son las *Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación*.

Conformidad

Legalex GS reclamará la conformidad con el presente documento aplicado en las políticas de sellos digitales de tiempo identificando en los certificados digitales y en la emisión de sellos digitales de tiempo que se provean bajo la TSA **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 sellos digitales de tiempo identificada dentro del certificado o sello que se emita bajo la TSA 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 interno o externo a la organización de Legalex GS, previamente identificado, que confirme que la TSA cumple con los requisitos de las políticas de sellos digitales de tiempo. Así mismo el Auditor no debe tener una relación jerárquica con el departamento que opera la TSA. 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 TSA conforme, demostrará que cumple con sus obligaciones tal y como se define en el título *Obligaciones de la TSA* de este mismo documento.
4. El PSC implementará los controles que cumplan con los requisitos de la Declaración de prácticas de Sellos digitales de tiempo.
5. Legalex GS puede emitir certificados de sello 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 Sellos Digitales de Tiempo, 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 Cámara de diputados del H. Congreso de la Unión y la Secretaría de Economía respectivamente, Legalex GS dejará de proveer y administrar sellos digitales de tiempo 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 TSA 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 TSA, se encargará de emitir, proveer y de administrar el servicio de emisión de sello digital de tiempo.

El proceso de generación de las llaves para las unidades de sellado de tiempo (TSU) se realizan bajo situaciones controladas. El servicio de validación de los sellos digitales de tiempo, proveídos por Legalex GS será accesible desde el portal <https://www.legalexgs.com>; verificar la validez y vigencia del documento sellado.

El sistema de TSA rechazará cualquier intento de emitir o proveer un sello digital de tiempo cuando el certificado de la TSA esté expirado o fuera de la vigencia.

Estampado de tiempo

El sistema TSA de Legalex GS cumplirá con los estándares señalados en el RFC 3628 para garantizar la calidad, el rendimiento y el funcionamiento del servicio de emisión de sello digital de tiempo.

El sistema TSA 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 sellado digital de tiempo.

El tiempo oficial UTC (Tiempo Coordinado Universal) se obtiene por medio de una sincronización con los servidores del Centro Nacional de Metrología (CENAM) por medio de una conexión segura y el protocolo NTP.

Token o identificador de Sello Digital de Tiempo

El token generado por la TSU de Legalex GS debe cumplir con las especificaciones técnicas del estándar RFC 3161 (IETF, 2018).

La estructura del TST (Token de Sello de Tiempo) contiene los siguientes elementos:

1. Un identificador de la política de la TSA.
2. Un número de serie único que permita identificar un sello digital de tiempo específico.
3. El tiempo, fecha y hora de generación, indicando la fuente de tiempo confiable.
4. La precisión definida del tiempo.
5. La representación del dato (Hash), provisto por el suscriptor para que sea sellado el o los datos.
6. La firma electrónica que ha sido generada usando una llave pública de la TSA.
7. La identificación de la TSA y de la TSU.

Para más información consulte la Declaración de prácticas de Sellado digital de tiempo.

Algoritmo de encriptación de datos

El sistema TSA 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 sello digital de tiempo. Para más información consulte la Declaración de prácticas de Sellado digital de tiempo en el tema Algoritmo de encriptación de datos.

Sincronización del reloj con la hora UTC

Legalex GS contrata el servicio de transferencia de hora segura con el Centro Nacional de Metrología (CENAM) quienes son los encargados de generar la Hora Oficial para los Estados Unidos Mexicanos en base a su escala de Tiempo Universal Coordinado UTC(CNM).

CENAM nos garantiza transferir la escala de tiempo UTC(CNM) a través de Redes Privadas Virtuales (VPN), con lo cual es posible mantener sincronizado al servidor de tiempo de Legalex GS al UTC por debajo de -100ms.

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 Sellos Digitales de Tiempo se lleven a cabo. El PSC también garantizará el cumplimiento de cualquier obligación adicional indicada en el servicio de sellos digitales de tiempo, ya sea directamente o incorporada por referencia. Otras obligaciones a las que está sujeta el PSC son:

1. Proporcionar el servicio de emisión de sellos digitales de tiempo de acuerdo con su declaración de práctica y la presente Política de sellos digitales de tiempo.
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 TSA sean ofrecidos mediante un sitio de alta disponibilidad.
4. Mantener los relojes de los sistemas de la TSU sincronizados mediante los protocolos establecidos con el CENAM.
5. Garantizar que los sellos digitales de tiempo emitidos o proveídos determinarán la fecha y la hora con la precisión establecida.
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 sellos digitales de tiempo, infraestructura de redes, seguridad, auditorías internas y cualquier otro necesario, tal como lo establecen las reglas generales a las que deben 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 sellos digitales de tiempo.

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 sellos digitales de tiempo.
10. Poner a disposición de los usuarios la Política de Sellos Digitales Pública, así como la Declaración de prácticas de sellos digitales de tiempo pública en el sitio <https://www.legalexgs.com>.
11. 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 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 sellos digital de tiempo.

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

Los términos, condiciones, uso y prácticas legales del servicio de emisión de sellos digitales de tiempo se encuentran detallados dentro del contrato de servicios de Legalex GS, donde se marcan las obligaciones de los suscriptores hacia el PSC y el uso de los sellos digitales de tiempo, entre las cuales se encuentran:

1. Conocer, entender y aceptar las Políticas y la Declaración de prácticas de Sellos Digitales de Tiempo de Legalex GS.
2. Conocer el propósito y el alcance de los sellos digitales de tiempo emitidos o proveídos por Legalex GS y usarlo únicamente para lo estipulado en la presente Política de Sellos Digitales de Tiempo.
3. En su caso, aceptar los términos y condiciones que le plantee Legalex GS.
4. Solicitar sellos digitales de tiempo únicamente desde las plataformas autorizadas por Legalex GS.
5. Verificar que el token recibido por parte del servicio de sello digital del tiempo 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 sello digital de tiempo emitidos por la TSA.

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 confían en los sellos digitales de tiempo de Legalex GS se atenderán a los términos y condiciones de la TSA las cuales estipulan:

1. Verificar que el token recibido por parte del servicio de sello digital del tiempo 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 los sellos digitales de tiempo emitidos por Legalex GS y usarlo únicamente para lo estipulado en la presente política de sellos digitales de tiempo.
3. Asegurar el uso de los sellos digitales de tiempo para los usos estipulados en el presente documento.
4. Notificar o dar aviso sobre cualquier situación considerada anómala con respecto a los servicios de sellos digitales tiempo y/o a los sellos digitales de tiempo emitidos o proveídos.

Responsabilidades del PSC

1. Garantizar el cumplimiento de las obligaciones descritas en el anterior segmento y de incumplirse por alguno de sus involucrados, buscar la sanción correspondiente.
2. Asegurar que los sellos digitales de tiempo que expida Legalex GS son válidos y va conforme se declara en este documento.
3. El token o identificador de sello digital de tiempo es único y va en respuesta a una sola solicitud de parte del suscriptor o cliente.
4. Cumplir con las revisiones y auditorías, así como acatar las recomendaciones que presenten los auditores para mejorar el servicio de la empresa.
5. Los sellos digitales de tiempo emitidos por la TSA de Legalex GS, deben usarse únicamente con las finalidades establecidas en la declaración de prácticas de sellos digitales de tiempo en su apartado de aplicabilidad.
6. Las Responsabilidades del PSC completas se integran en el contrato de servicios.
7. Negar o limitar cualquier responsabilidad a menos que se estipule lo contrario por la ley aplicable.

Responsabilidades de los suscriptores

1. Resguardar los archivos que se dan como efecto de cada SDT y de administrar sus propias copias de seguridad de los archivos que sellen y los archivos provenientes de.
2. Mantener un uso correcto de sus credenciales para el servicio de SDT, 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 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 SDT en el tema Responsabilidades de los suscriptores.

Descarto de responsabilidades

Mediante la *Declaración de Prácticas de Sellos Digitales de Tiempo*, 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 SDT en el tema Descarto de Responsabilidades.

Limitaciones del servicio

El servicio de emisión de sellos digitales de tiempo 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 la PSC.

El PSC se reserva la responsabilidad de garantizar la validez de un token o identificador de sello digital de tiempo más allá del final del período de validez del certificado emitido para la TSA.

Responsabilidades Económicas

Las responsabilidades económicas a las que la TSA 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 exhibe una irresponsabilidad. Para más información consulte el Tema de Responsabilidades Económicas dentro de la Declaración de prácticas de Sellos digitales de tiempo.

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
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 140-2	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 Standards 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)
ITU-T	Siglas del Sector de Normalización de las Telecomunicaciones de la Unión de telecomunicaciones. (ITU, 2017)
NIST	Acrónimo de National Institute of Standards and Technology. (NIST, National Institute of Standards and Technology, 2001)
NTP	Acronimo de Network Time Protocol, Es el protocolo que se utiliza para sincronizar los relojes de los sistemas informaticos. (Wikipedia, 2018)
NTPD	Network Time Protocol Daemon.
PSC	Prestadora 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)
RFC	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)
SE o S.E.	Secretaría de Economía
TSA	Autoridad de sellado de tiempo (RFC 3628, 2018)
TSU	Unidad de sellado de tiempo (RFC 3628, 2018)
UTC	Tiempo Universal Coordinado

Tabla 4Acrónimos

Glosario

Definición	Significado
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)
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)
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, incluyendo cualquier otro servicio brindado por una PSC. (Secretaría de Economía, 2008)
Suscriptor	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.
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 5Definiciones

Apéndice B

Bibliografía

- C, M. S. (05 de Febrero de 2006). *Tecnologías de la información y procesos de negocio (BPM)*. Obtenido de ¿Qué son los Web services?: <https://msaffirio.wordpress.com/2006/02/05/%C2%BFque-son-los-web-services/>
- ETSI. (01 de Enero de 2017). *ETSI*. Obtenido de ETSI: <http://www.etsi.org/>
- IETF. (25 de Marzo de 2015). *IETF Org*. Obtenido de The goal of the IETF is to make the Internet work better: <https://www.ietf.org/>
- IETF. (30 de Mayo de 2018). *RFC 3161*. Obtenido de RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP): <https://tools.ietf.org/html/rfc3161>
- International Organization Standards. (s.f.). *International Standards--CCITT Recommendation X. 660 (1992) | ISO/IEC 9834-1: 2. Information technology--Open Systems Interconnection--Procedures for the operation of OSI Registration Authorities: General procedures, 8824*.
- ITU. (01 de Enero de 2017). *El UIT-T en breve*. Obtenido de ITU: <http://www.itu.int/es/ITU-T/about/Pages/default.aspx>
- Microsoft azure. (01 de Enero de 2012). *¿Qué es un middleware?* Obtenido de <https://azure.microsoft.com/es-mx/overview/what-is-middleware/>
- NIST. (30 de Mayo de 2018). *NIST*. Obtenido de NIST FIPS 180-4 Secure Hash Standard (SHS): <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf>
- NIST, National Institute of Standards and Technology. (25 de Mayo de 2001). *Security requirements for cryptographic modules*. Gaithersb, Condado de Montgomery, Maryland. Obtenido de <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf>
- Porras, A. (20 de Junio de 2015). *Qué son los tokens de seguridad y cómo funcionan*. Obtenido de Blog Soporte para PC: <http://www.soporteparapc.com/2015/06/que-son-tokens-de-seguridad-y-como-usar.html>
- RedHat INC. (02 de Enero de 2017). *Cifrado de llave pública*. Obtenido de RedHat documentación, guía de seguridad: https://access.redhat.com/documentation/es-ES/Red_Hat_Enterprise_Linux/6/html/Security_Guide/apas02.html
- RFC 3628. (24 de 06 de 2018). *IETF Tools*. Obtenido de Policy Requirements for Time-Stamping Authorities: <https://tools.ietf.org/html/rfc3628>
- Safenet. (01 de Junio de 2015). *Hardware security modules (HSM)*. Obtenido de Safenet, Gemalto security to be free: <http://www.safenet-inc.es/data-encryption/hardware-security-modules-hsms/>

Secretaría de Economía. (05 de Marzo de 2007). Acuerdo de las Reglas generales a las que deberán sujetarse los prestadores de servicios de certificación. *Diario oficial de la federación*, págs. 1-21.

Secretaría de Economía. (01 de Junio de 2008). *Firma digital PSC*. Obtenido de Firma digital PSC: <http://www.firmadigital.gob.mx/psc2.pdf>

Secretaría de Gobernación SEGOB. (11 de Enero de 2012). *Ley de firma electrónica avanzada*. Obtenido de Diario oficial de la Federación: http://www.dof.gob.mx/nota_detalle.php?codigo=5228864&fecha=11/01/2012

Wikipedia. (01 de 08 de 2018). *Network Time Protocol*.