LEGALEX GS®

Declaración de Prácticas de Sellos Digitales de Tiempo

Para el Sellado digital de tiempo

OID: 2.16.484.101.10.316.100.6.1.3.2.1

VERSIÓN PÚBLICA

PSC LEGALEX GS SA de CV

Morelia, Michoacán 2018

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

DECLARACIÓN DE PRÁCTICAS DE SELLOS DIGITALES DE TIEMPO VERSIÓN PÚBLICA
LEGALEX GS, S.A. DE C.V.

OID: 2.16.484.101.10.316.100.6.1.3.2.1

LEGALEX GS S.A. DE C.V.

RFC LGS160502EA8

LEGALEX GS S.A. DE C.V.

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

FECHA DE INICIO DE OPERACIONES
LEGALEX GS opera como PSC desde 20 de Junio de 2019.

Tabla de contenido

Tabla de cuadros y esquemas

Tabla de ilustraciones

Identificación del documento

En esta sección se identifican los datos principales del documento:

Nombre	Declaración de Prácticas de Sellos Digitales de Tiempo versión Pública
Versión	1.1
Autor	Legalex GS.
Estado	Terminado.
Fecha de elaboración	15 de Octubre del 2018
Fecha de actualización	10 de junio de 2019
OID (Identificador digital)	2.16.484.101.10.316.100.6.1.3.2.1

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 es el Profesional Informático de Legalex GS.

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

Tabla 3Autorización

Presentación de la PSC

Legalex GS es un órgano interlocutor entre las personas que necesitan el uso de los sellos digitales de tiempo 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 los sellos digitales de tiempo, en conjunto con los términos y los requisitos que establece el Código de comercio y las Reglas a las que deberán sujetarse los PSC.

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 los sellos digitales de tiempo sobre todo en el ámbito público y en los medios electrónicos que la puedan conformar donde se tendrán que reconocer los medios de prueba.

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 los sellos digitales de tiempo 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 sellado de tiempo 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 del servicio de emisión de sello digital de tiempo y sus complementos, mantener la seguridad tanto del personal que labora como de los datos sensibles que se manejan y proveer la estructura organizacional que presenta la TSA.

Introducción

El presente documento contiene la *Declaración de Prácticas de Sellos Digitales de Tiempo*, de la Autoridad de Sellado de Tiempo (TSA) Legalex GS S.A. de C.V. Donde se establecen términos y condiciones, así como las prácticas comerciales y operativas para llevar a cabo la prestación de servicios fiables de sellos digitales de tiempo.

La declaración de práctica de Sellos Digitales de Tiempo es más específica que una política de sello de tiempo. Una declaración de práctica de SDT es una descripción más detallada de los términos y condiciones, así como las prácticas comerciales y operativas de una TSA en la emisión o provisión y administración de servicios de sellado de tiempo.

El servicio de emisión de sello digital de Tiempo ofrecidos por Legalex GS están regidos por *las "Reglas generales a las que deberán sujetarse los Prestadores de Servicios de Certificación", Regla 118,* 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)*" en sus capítulos 4 y 7.

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

1. Los procedimientos de operación para otorgar y proveer un sello digital de tiempo y el alcance de estos.
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 sellos digitales de tiempo.
4. Controles que se utilizarán para asegurar las auditorías y el almacenamiento de información relevante.
5. Compatibilidad con el RFC 3628 en su capítulo 4 "General concepts" y 7 "Requirements on TSA practices".
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 TSA de Legalex GS con respecto al servicio de emisión y validación de sellos digitales de tiempo.

Conceptos generales

Servicios del 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 digital de tiempo, 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 sello digital de tiempo para las firmas electrónicas, especialmente 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 del servicio de emisión de 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 digital, este componente es público y se encarga de validar que el sella digital de tiempo en un archivo es válido.

Interacción de los servicios

Emisión de sello digital de tiempo

Actualmente en la PSC Legalex GS, contemplamos dos esquemas para el consumo del servicio de emisión de sellos digitales de tiempo, los cuales constan de:

- Peticiones cliente a cliente.
- Uso de nuestra plataforma (consumo del SDT mediante el cliente de la TSA).

Petición cliente-cliente

El sellado de tiempo digital cliente-cliente consta que una aplicación cliente externa al aplicativo cliente de TSA (Legalex TSA) se conecte y haga peticiones del servicio sin que intervengan las interfaces del propio aplicativo del TSA que administra las peticiones (Legalex TSA), el proceso de sellado de tiempo digital se efectúa de la siguiente manera:

1. Cotización del servicio directamente con el Director ejecutivo.
2. Entregar documentación requerida (razón social, RFC, pagos, copias de identificaciones oficiales, comprobante de domicilio y poder del

representante legal en caso de ser moral) y celebrar el contrato de servicios sobre la emisión de sello digital de tiempo 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 al sistema que se les proporcionen para el uso del servicio de SDT.
4. Una vez establecidas las conexiones entre el sistema del cliente y el cliente de la TSA de Legalex GS, realizar las pruebas correspondientes.
5. Al efectuarse la petición del servicio de emisión de sello digital de tiempo, se hace la petición a la TSA de Legalex GS para el servicio de emisión del sello digital de tiempo.
6. Durante el proceso del SDT regresa un objeto tipo token.
7. Una vez terminado el proceso de SDT el middleware regresa el resultado final del documento que se selló en conjunto con dos archivos que son el respaldo de que la operación fue exitosa al cliente.
8. Una vez terminado el proceso del sellado se actualiza la base de datos de la TSA con la fecha, hora y hash de sello, regresando el resultado de la petición a la aplicación cliente que la solicito.
9. Cuando termine la operación, la aplicación cliente del TSA actualiza a la redundancia.

Cabe mencionar que cada aplicativo de cliente externo a Legalex GS, se le mandarán los archivos como resultado del servicio de emisión de sello digital de su solicitud de sello y cada desarrollador del aplicativo se responsabilizará de hacerle llegar estos archivos a su cliente final o utilizarlos según sus propias políticas.

Emisión del SDT mediante el cliente de la TSA

La emisión del sello de digital de tiempo también se podrá realizar mediante un aplicativo cliente que se conecta directamente a la TSA 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 el SDT y en ese mismo sitio podrán descargar el resultado de la operación del SDT, teniendo los siguientes pasos a realizar:

1. Cotización del servicio a través del Director ejecutivo.
2. Entregar la documentación requerida (razón social, RFC, pagos, copias de identificaciones oficiales, comprobante de domicilio y poder del representante legal en caso de ser moral) y celebrar el contrato de servicios sobre la emisión del sello digital de tiempo 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 SDT.
4. Acceder a la plataforma o sitio web donde podrá realizar las operaciones de emisión de sello digital de tiempo https://www.legalexgs.com/legalex_tsa, subir los archivos que serán sellados y hacer la petición de emisión de sello digital de tiempo una vez terminado de subir los archivos.

5. Una vez realizada la petición esta viajará hasta ser recibida por la TSU quien sellará las operaciones de SDT.
6. Sí estas peticiones son correctas, se hace la solicitud del SDT a la TSA la cual se encargará de firmar la petición mediante la TSU. Así mismo la TSU hará la petición al servicio de tiempo (reloj) para corroborar la fecha y hora de la operación. El servidor del tiempo está sincronizado con el servicio de tiempo seguro proporcionado por el CENAM.
7. Una vez terminado el proceso de SDT se regresa el resultado final del documento que se selló en conjunto con dos archivos que son el respaldo de que la operación fue exitosa al aplicativo cliente de la TSA.
8. Queda almacenada la operación en la base de datos del cliente de la TSA. Estos archivos son recibidos y almacenados dentro del cliente de la TSA, registrando la operación y los archivos originales en conjunto de los respaldos de operación del SDT.
9. El cliente o suscriptor final obtiene, descarga y visualiza su petición ya sellado en conjunto con sus respaldos.

Validación del SDT

La validación del SDT se realiza a través de la página de Legalex GS, entrando al siguiente URL de forma pública: https://www.legalexgs.com/servicios/sellos/validar.jsp donde los clientes o suscriptores finales tendrán que seguir los siguientes pasos:

1. El suscriptor deberá subir el archivo original y los archivos que respaldan el SDT (archivos .tsr y .tsq).
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 TSA, 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 TSA, valida que el certificado sea el mismo con el que fue sellado y así mismo el hash del SDT.

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

Entidades participantes en la infraestructura de sello digital de tiempo

Existen actores y entidades que participan dentro de la infraestructura de sello digital 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.

3. 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.
4. Los suscriptores o entidades finales, es decir, las personas u organizaciones que solicitarán el servicio de emisión de sello digital de tiempo, que podrían también llamarse "solicitantes".
5. Terceros que confían, son aquellos que expresan su "fe" en la Autoridad de Sellado de Tiempo al creer que sus servicios son lo suficiente confiables. Por lo general, estos suelen ser también subscriptores, pero no necesariamente debe ser así.

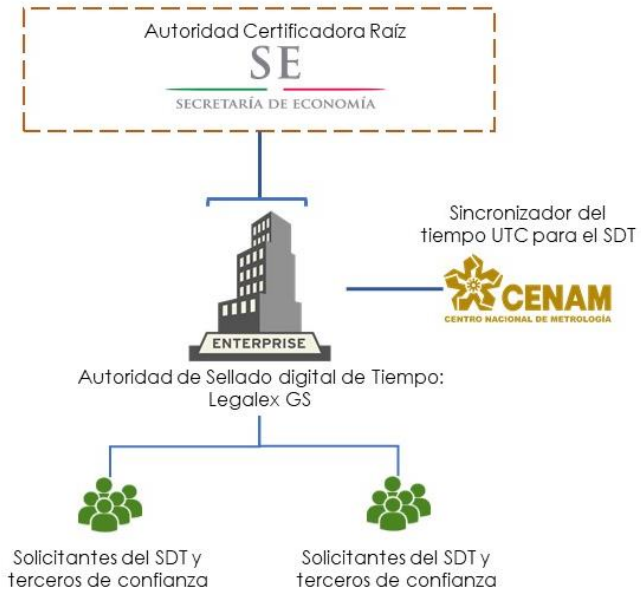

Ilustración 1Escalonamiento de la ASDT

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 sellado de tiempo realice. TSA tiene la responsabilidad de llevar a cabo correctamente el servicio de emisión de sellado de tiempo que se nombran en el tema *Servicios del Sello digital de tiempo* dentro de este documento.

La TSA es responsable de la operación de la unidad de sellado digital de tiempo (TSU), es decir, las transacciones que se crean y firman en nombre del TSA y el suscriptor o receptor de la transacción. La TSA responsable para emitir un token de sello digital de tiempo está configurada para incluir en el token de sello digital de tiempo la hora mediante un servidor de tiempo, que está sincronizada con el Centro Nacional de Metrología (CENAM), 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.

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. El conjunto de estos elementos permite demostrar que una serie de datos han existido y no han sido alterados desde un instante de tiempo específico y confiable, siempre y cuando cumpla los requisitos para recibir el servicio de emisión de sello digital de tiempo, entre los cuales comprende:

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

Otros aspectos importantes 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. La PSC mantendrá informado a los suscriptores o usuarios finales del servicio de las responsabilidades que se tendrán bajo esté servicio, así como, en caso de que la PSC sea suspendida o corrompa una ley, las acciones que llevará a cabo la PSC para subsanar el daño que pueda presentarse a sus suscriptores y clientes.
4. Cuando el suscriptor es un usuario final, el usuario final será considerado directamente responsable cuando sus obligaciones no se cumplan correctamente.

Requisitos de las prácticas del PSC.

El PSC implementa controles para cumplir con los requisitos del servicio de emisión de sello digital de tiempo. Estos requisitos no implican alguna restricción para ofrecer los servicios de la TSA.

La provisión de un token o identificador de sello de tiempo en respuesta a una solicitud queda a moderación del PSC según los acuerdos de nivel de servicio que se establecen en la política de SDT y en el presente documento.

Declaración de prácticas y divulgación de la TSA

Declaración de prácticas de la TSA

Dentro de la Declaración de prácticas de SDT, el PSC se asegura que se demuestra la integridad necesaria para proporcionar el servicio de emisión de sello digital de tiempo. En particular se describe lo siguiente:

1. El PSC expone ante la S.E. el documento de Análisis y Evaluación de Riesgos y Amenazas tal y como se especifican las Reglas a las que deberán sujetarse los PSC, regla 98. Dicho documento especifica las vulnerabilidades que pueden afectar a los activos de la TSA 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 Sellos Digitales de Tiempo*. El cual aborda los requisitos para ofrecer los servicios, según la regla 118 de las Reglas 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 la declaración de práctica de SDT y las políticas de sellos digitales de tiempo, para evaluar el cumplimiento de las políticas de sello digital de tiempo como se especifica en las Reglas a las que deberán sujetarse los PSC, regla 115.
5. La declaración y las políticas de SDT, así como toda la documentación pertinente es revisada y aprobada por la Secretaria de Economía, así como por el PSC de Legalex GS.
6. En el Apéndice C se establece un calendario de revisión para mantener las políticas y la declaración de prácticas actualizadas.
7. Cualquier cambio que surja y que impacte en las funciones/servicios de Legalex GS, deberán de ser notificados con la debida antelación a la Secretaria 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 sellos digitales de tiempo, así como el aviso de privacidad y los términos y condiciones relacionados con el uso del servicio de emisión de sello digital de tiempo a través de su sito electrónico:

https://www.legalexgs.com.

Para cada sello digital de tiempo que sea proveído por parte de la TSA de Legalex GS se especifican 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. El algoritmo Hash con el que se representan los datos del sello de tiempo. El cual corresponde al SHA-256 según las políticas de sello digital de tiempo.
3. 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 SDT firmado por el cliente/suscriptor que lo contrata.
4. 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 118 numeral II y conforme lo dicta el RFC 3628 sección 6.2 y 6.3.
5. Para verificar la información y validación del sello digital de tiempo donde las partes que confían puedan acceder a verificar el estado del sello, cumpliendo con el RFC 3628 sección 6.3 y el tema 7.1.2 inciso i): https://www.legalexgs.com/servicios/sellos/validar.jsp.
6. El período de conservación de los registros y documentos que se expiden de la contratación del servicio de SDT y los sucesos de TSA por parte de los suscriptores tendrá un tiempo de conservación de **10 años,** a partir de la firma del contrato.
7. 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 TSA

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 TSU se realizan bajo situaciones controladas y seguras.
2. Para la generación de las claves se realiza como se especifica en el RFC 3628, tema 7.2.1 inciso B. Cumpliendo así con la Regla 94, 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 TSA y la TSU será RSA con SHA256, empleando una longitud de clave de 4096 bits.

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

1. Generación de certificado de SDT por primera ocasión: Se solicitará la emisión del certificado de SDT que avale a Legalex GS como prestador de servicios de certificación.

2. Generación de certificado por renovación de vigencia: Una vez que la TSA haya comenzado a operar y la vigencia del certificado emitido por Secretaría de Economía esté próximo a caducar.
3. Generación de certificado de ASDT por revocación: Se solicitará de manera inmediata la emisión de un nuevo certificado de ASDT para la TSA que reemplace y anule el certificado anterior.

Protección de la clave privada del TSU

Las claves criptográficas deben estar disponibles operativamente tanto tiempo como lo requiera el servicio criptográfico correspondiente de la TSA (es decir, durante todo su ciclo de vida, el cual es de 10 años).

Resumiendo:

1. La clave pública de la TSU se conservará y se utilizará dentro del entorno de la TSA, que cumple con todas las especificaciones marcadas en la RFC 3628 tema 7.2.2 inciso a, y estarán disponibles a los terceros de confianza mediante la copia del certificado y su clave publica en nuestro sitio web.
2. En caso de que la clave privada se encuentre comprometida se procederá a ejecutar el proceso necesario para obtener un nuevo certificado para el servicio de emisión de sello digital de tiempo.

Distribución de la clave pública de la TSU

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

Renovación (nueva emisión) de las claves de la TSA

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

Fin del ciclo de vida de las claves de la TSU

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

Gestión del ciclo de vida del módulo criptográfico usado para el sellado digital de tiempo

Legalex GS utilizará módulos que cuenten con certificación FIPS 140-2 Nivel 3, protegido por contraseña y múltiples factores de seguridad. Cumpliendo así con la

regla 94, numeral II de las Reglas generales a las que deberán sujetarse los PSC. Aseguraran en conjunto con la TSA los siguientes puntos:

1. El PSC garantizarán la seguridad, mantenimiento y el correcto funcionamiento de la seguridad del módulo criptográfico a lo largo de su ciclo de vida.
2. El dispositivo se localiza en el lugar más seguro dentro del centro de datos que garantiza un entorno físico seguro, al que únicamente pueda acceder personal autorizado.
3. La instalación y activación de las claves de firma de la TSU en el Servidor de tiempo serán realizadas exclusivamente por el personal con funciones de confianza.
4. La clave privada de firma de la TSU será borrada al momento de que sea retirada del dispositivo criptográfico.

Sobre el estampado de tiempo

La TSA 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 sellado de tiempo.

Token o identificador de Sello Digital de Tiempo

El token generado por la TSA de Legalex GS debe cumplir con las especificaciones técnicas del estándar RFC 3161 (IETF, 2018). Además, la TSA asegurará que los identificadores del SDT se emitan de forma segura e incluyan la hora correcta que se sincroniza con el CENAM por medio de un protocolo NTPD.

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 estampar el tiempo.

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.

La sincronización con los servidores de Legalex GS se realiza por medio de un canal seguro VPN el cual es contratado con el CENAM y posteriormente se utiliza el protocolo NTP para la sincronización.

En caso de detectar anomalías, el servidor deberá de registrarlo en la bitácora y el profesional informático deberá de generar la petición de transferencia de la hora al CENAM por medio de NTP.

Por otro lado, Legalex GS es el responsable de la correcta sincronización del reloj utilizado por la TSU para el servicio de emisión de sellos digitales de tiempo.

Vigencia del sello digital de tiempo

Legalex GS establece la vigencia de los certificados para SDT en función del periodo de vigencia de las claves de la TSA que otorga la SE (10 años).

Gestión y operación del SDT

Requerimientos para operar el servicio

Las personas físicas o morales que requieren los servicios proporcionados por la Autoridad de Sello Digital de Tiempo y que aceptan explícita o implícitamente sus términos y condiciones establecidos en un contrato de prestación de servicios que deberán de contar con los siguientes requerimientos:

1. Contratación del servicio de SDT.
2. Una aplicación cliente compatible con el RFC 3161 Time-Stamp Protocol (TSP).
3. Acceso a internet mediante un navegador web compatible (Chrome, Firefox, safari).
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.

Así mismo el 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:

1. El PSC retendrá la responsabilidad de la prestación de servicios de SDT dentro del alcance que marca la presente declaración de prácticas de SDT y las políticas de SDT.
2. La dirección o el director ejecutivo de Legalex GS deberá proporcionar y hacer cumplir en conjunto con el profesional informático y el auxiliar 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.
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 TSA, marcados por el centro de datos de TRIARA, así mismo mantener documentados, actualizados y asegurados los controles de seguridad.

6. La PSC y la TSA se deberán de asegurar de que se mantenga la seguridad en la información cuando la responsabilidad de las funciones de la TSA sea subcontratada u otra organización o entidad.

Clasificación y gestión de activos

El PSC retendrá la responsabilidad de todos los aspectos de la prestación de servicios de sellado de tiempo dentro del alcance de este. Las responsabilidades de terceros serán claramente definidas por el PSC y los arreglos apropiados hechos para garantizar que los terceros estén obligados a implementar cualquier control requerido por el PSC. El PSC deberá retener la responsabilidad de la divulgación de prácticas relevantes de todas las partes.

La infraestructura de seguridad de la información necesaria para gestionar esta seguridad dentro de la TSA se mantendrá en todo momento según lo especificado en el sistema de gestión de seguridad de la información que está basado en el estándar ISO/IEC 27001.

El PSC también asegurará los siguientes:

1. El PSC conservará la responsabilidad de todos los aspectos de la provisión de servicios de sellado de tiempo dentro del alcance de la Declaración de prácticas del sellado digital de tiempo y la política de sello digital de tiempo, independientemente de si las funciones se subcontratan.
2. Las responsabilidades de terceros estarán claramente definidas por el PSC y los arreglos apropiados realizados para garantizar que los terceros estén obligados a implementar los controles requeridos por el PSC.
3. La dirección del PSC debe proporcionar orientación sobre la seguridad de la información a través de un foro de dirección de alto nivel que sea responsable de definir la política de seguridad de la información de la TSA.
4. La infraestructura de seguridad de la información necesaria para gestionar la seguridad dentro de la TSA se mantendrá en todo momento. Así como se prevé en el Sistema de Gestión de Seguridad de la información basado en la ISO/IEC 27000.
5. Se documentarán, implementarán y mantendrán los controles de seguridad y los procedimientos operativos para las instalaciones, sistemas y activos de información del PSC que brindan los servicios de sellado de tiempo.
6. Debe describir las reglas, directivas y procedimientos con respecto a cómo se otorgan los servicios especificados y la garantía de seguridad asociada, además de establecer políticas sobre incidentes y desastres, como se especifican en el Plan de continuidad del negocio y respuesta ante desastres.

Solicitud de servicio

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

1. Agendar una cita mediante el 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 sellos digitales de tiempo.
5. Guardar y cuidar las credenciales de acceso que se le den para comenzar el uso del servicio de SDT.

Gestión y clasificación de los activos

Legalex GS en cumplimiento de las reglas generales a las que deben sujetarse los prestadores de servicios de certificación, realizó un Análisis y Evaluación de Riesgos y Amenazas (AERA), en el cual se detalla sobre los activos críticos con los que cuenta la PSC y los riesgos detectados asociados a dichos activos, además dentro del plan de seguridad de sistemas se detalla un inventario completo de los activos de la PSC.

Seguridad del personal

El PSC se asegurará de que el personal contratado cumple con las especificaciones que establece la SE, considerando lo siguiente:

1. El PSC deberá emplear personal que posea el conocimiento experto, la experiencia y las calificaciones necesarias para los servicios ofrecidos y según corresponda a la función laboral.
2. Las funciones y responsabilidades de seguridad, tal como se especifica en la política de seguridad de la ASDT.
3. El personal del PSC deberá tener descripciones de trabajo definidas en sus contratos laborales, funciones y niveles de acceso.
4. El personal deberá ejercer los procedimientos y procesos administrativos y de gestión que estén en línea con los procedimientos de gestión de seguridad de la información del PSC.

Los siguientes controles adicionales se aplicarán a la administración de sellado de tiempo:

1. Se deberá emplear al personal de confianza con más alto rango que posea:
    a. Conocimiento de la tecnología de sello digital de tiempo.
    b. Conocimiento de la tecnología de firma digital.
    c. Conocimiento de los mecanismos de calibración o sincronización de los relojes de la TSU con UTC.
    d. Familiaridad con los procedimientos de seguridad para el personal con responsabilidades de seguridad.
    e. Experiencia con seguridad de la información y evaluación de riesgos.

f. Todo el personal del PSC en funciones de confianza deberá estar libre de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones de la TSA.

2. El personal del PSC debe ser nombrado formalmente para funciones de confianza por la alta gerencia responsable de la seguridad.
3. El PSC no asignará a funciones de confianza o de gestión a ninguna persona que se tenga conocimiento que tiene condena por un delito grave u otra ofensa que afecta su idoneidad para el puesto. El personal no tendrá acceso a las funciones de confianza hasta que se completen las verificaciones necesarias.

Sobre el control de seguridad del personal

Legalex GS declara los siguientes enunciados como comprobaciones de seguridad sobre el personal para efectos de seguridad:

1. El PSC definirá las tareas específicas de cada individuo y sus responsabilidades.
2. El PSC realizará la verificación de cada persona que selecciono para un puesto en específico.
3. Las obligaciones correspondientes a cada individuo son seleccionadas por el PSC.
4. El PSC se hace responsable de las buenas prácticas que se realizan como apoyo a la validez de confianza hacia el individuo, como exámenes, actos de buena fe.
5. Las operaciones que se realicen adentro de la prestadora de servicios y que involucren a la infraestructura de clave pública, están protegidas por un contrato de confidencialidad, al ser violado, el PSC tiene el derecho de atacar mediante un juicio al personal responsable de la divulgación.
6. El PSC se guarda el derecho de contratación a personas que poseen antecedentes penales.

Proceso de Reclutamiento

El proceso de reclutamiento corre a cargo del Director Ejecutivo con el apoyo del personal de Legalex GS, en caso contrario el Director Ejecutivo contratará una empresa externa para el apoyo del reclutamiento de los recursos humanos necesarios. Este proceso viene detallado en el documento Titulado *Proceso de reclutamiento de Legalex GS*.

Seguridad física y ambiental

LEGALEX establece una serie de controles de acceso para asegurar los servicios críticos y minimizar los riesgos. En este sentido, dentro de las políticas de seguridad de la información se detallan las políticas para el control de acceso, ya sea a las oficinas principales (por parte de personal empleado, clientes o proveedores) o en los centros de datos que son los que contienen los activos críticos para la organización.

Gestión de controles físicos

Legalex GS, se asegurará que todo acceso físico hacia los principales servicios críticos, como el servicio de redes y bases de datos, sean controlados y analizados frecuentemente; para la reducción de posteriores riesgos físicos a los activos y datos que estos servicios manejan en sus canales de comunicación.

Sobre el acceso físico

La seguridad y el acceso físico a las oficinas administrativas de Legalex GS está gestionado mediante controles de acceso biométricos que sólo permiten el ingreso a los usuarios a las áreas asignadas por autorización de la dirección. En las oficinas solo se resguardarán:

1. Documentación de identificación de los solicitantes o suscriptores.
2. Computadoras para el personal de las áreas administrativas y sistemas.

El acceso a las diferentes áreas está restringido a través de un acceso. Dichos controles deberán ser acatados tal y como se estipulan en las políticas de seguridad de la información de Legalex GS.

Sobre la Destrucción de documentos

Todo aquel documento, llámese impreso, nota del momento, recado, post-it, expediente, etc. Que se encuentre mediante una hoja de papel y contenga información relacionada con el servicio de Emisión de Sellos Digitales de Tiempo, clientes, información sensible sobre los datos, mensajes de datos y su conservación, confidencial o de orden mayor serán eliminados de forma definitiva e incorregible en los siguientes casos:

1. La TSA o PSC Legalex GS deje de existir.
2. Sea o se encuentre bajo estado de suspensión definitiva.

Gestión de operaciones

Legalex GS, se asegurará de que los componentes del sistema TSA sean seguros y funcionan correctamente, con un riesgo mínimo de falla. Para ello, realiza las siguientes acciones:

- Para reducir la probabilidad de que los equipos de cómputo sean infectados por software malicioso, todo equipo de cómputo debe tener instalado un software antivirus y revisar diariamente si existe alguna actualización de su BD. Y finalmente se tiene prohibido la instalación de software no licenciado y que no tenga que ver con las actividades que se desarrollan por el usuario.
- Los medios utilizados dentro del sistema de la TSA se manejan de forma segura para proteger los medios de daños, robos, accesos no autorizados y obsolescencia.

- Toda la información que contenga datos confidenciales y que se generen a partir del servicio de emisión de sellos digitales de tiempo. Deberán de mantenerse seguros en el archivero, el cual se encuentra aislado por puertas de acceso biométrico y cámaras de circuito cerrado.
- La PSC Legalex GS actuará de manera oportuna y rápida para responder a cualquier incidente que se presente en los activos informáticos, tal y como se especifica en el manual de plan de respuesta ante desastres.

Gestión de acceso a los sistemas

El acceso al sistema TSA de Legalex GS, tanto hardware como software, está limitado al personal autorizado.

Legalex GS proporciona seguridad a los equipos del sistema TSA mediante las siguientes especificaciones:

1. Todos los servicios que se proporcionen están protegidos.
2. Canales seguros.
3. Listas de controles de acceso.
4. Antivirus actualizado.
5. Software controlador, de monitoreo y administrador de servicios.
6. Redes privadas y segmentadas.
7. Restricción de puertos y servicios de red.

Los detalles de las acciones relacionadas a los accesos a los sistemas se describen en las Políticas de Seguridad de la Información y el Plan de seguridad de sistemas.

Mantenimiento e implementación de sistemas de confianza

De la misma forma Legalex GS, asegura que todo aquel sistema desarrollado por su personal es seguro y se administra de forma correcta bajo los estándares requeridos en la presente declaración de prácticas de SDT y en las Reglas generales a las que deberán sujetarse los PSC marcadas por la Secretaría de Economía, por lo que se hace el supuesto que existe un riesgo minúsculo de fallo. Por lo cual, cualquier daño, perjuicio o incidente de seguridad, que sea producido por un mal funcionamiento o mal manejo de las plataformas queda arraigado a las autoridades actuales y presentes, para la dimensión de la sanción oportuna.

Así mismo, se plantea que la forma más rápida para la resolución de los problemas, iniciándose de la siguiente forma:

1. Identificar el problema con rapidez.
2. Proporcionar toda la información necesaria, importante y descriptiva del riesgo o problema que pudo haberse presentado.
3. En caso de haber registrado alguna solución y que esta fuese fallida, también se deberá reportar.
4. En caso de no haber solución, toda esta información adquirida debe de ser notificada.

5. Plasmar toda la información en la bitácora de *Registros de eventos no deseados* y registrar así mismo la solución que se le dio, esto con el fin de complementar y madurar aún más los manuales" Plan *de continuidad del negocio y respuesta ante desastres*".

Compromiso de los servicios del PSC

En caso de que la clave privada de una TSU/TSA se vea comprometida, Legalex GS, procederá a notificar a la SE, revocar el certificado de la TSU/TSA y evitar la emisión de sellos de tiempo firmados por dicho certificado, posteriormente se procederá a la solicitud de una nueva emisión de un certificado para reanudar las operaciones de la TSU/TSA lo más pronto posible.

Si existe evidencia o sospecha de pérdida de calibración de los relojes de las TSU, las TSA no emitirá ningún sello digital de tiempo hasta corroborar la recalibración y notificará a las partes interesadas que pudieran haber solicitado y recibido un sello digital durante el percance.

Terminación y Sucesión de la ASDT

En caso de la suspensión o disolución de la Autoridad de Sellado de Tiempo, 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 del PSC:

1. Notificar a las autoridades o personal competente de la salida, baja o disolución del 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 TSA 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 laboro en las oficinas será debidamente conservada y resguardada para auditorias 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 del PSC.
4. El PSC que continúe con las operaciones de la TSA 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 alterno 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 TSA de Legalex GS, procurara 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. El PSC procurara 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 TSA de Legalex GS finalice sus servicios de SDT de ser el caso, ejecutará como mínimo:

1. Pondrá a disposición de sus suscriptores y terceros de confianza la información sobre su terminación.
2. El PSC dará por terminada la autorización de todos los subcontratistas para actuar en nombre del PSC en el desempeño de cualquier función relacionada con el servicio de emisión de sellos digitales de tiempo.
3. El 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 TSA por un periodo razonable.
4. El PSC mantendrá o transferirá a una parte confiable (otra PSC con TSA o a la Secretaría de Economía) su obligación de poner a disposición su clave pública o su certificado de SDT a partes confiables por un tiempo razonable.
5. Las claves privadas de la TSU y TSA, incluidas las copias de seguridad, se destruirán de una manera tal que las claves privadas no puedan ser recuperadas.
6. El 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. El 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 Sellado de Tiempo, 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 deben sujetarse los Prestadores de Servicios de Certificación establecido por la Secretaria de Economía, además, la TSA 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 sello digital de tiempo

Legalex GS, mantiene registros de las operaciones relacionadas con la solicitud, contratos, servicio y otros aspectos relacionados con la provisión de sellos digitales.

Obligaciones y responsabilidades

Obligaciones

Obligaciones del PSC

La PSC de Legalex GS, se asegurará de que todos los procedimientos detallados en la presente Declaración de Prácticas de Sellos Digitales de Tiempo.

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 que cuando 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 estable las reglas generales a las que deben sujetarse las 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 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 S.E. 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 Publica, 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 digitales de tiempo.
13. Emitir SDT conforme a la presente declaración de prácticas, las políticas de sellado digital de tiempo y con la información que el suscriptor proporciono en el momento que se requirió para la elaboración del contrato de servicios prestados por la PSC de Legalex GS.
14. La conservación por medios electrónicos de información y documentos que se relacionen con los sellos digitales de tiempo emitidos, así como los contratos de servicios durante al menos el lapso de 10 años desde su expedición, serán responsabilidad del encargado de resguardo.
15. Los datos que se transmiten entre los sistemas o plataformas (toda información delicada) son usados y enviados sobre una conexión segura (VPN).
16. El 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.
17. Brindar y prestar los servicios relacionados con la emisión de sellos digitales de tiempo.
18. La contratación específica y de perfil adecuado del personal que se encargará de asegurar la calidad del servicio.
19. Declaramos que queda estrictamente prohibido la reventa y copias no autorizadas del servicio de emisión de sellos digitales de tiempo de Legalex GS por un tercero.

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.

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 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.
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 del sello digital de tiempo para evitar el mal uso de un documento ya sellado.
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 firmo con Legalex GS.
14. Utilizar de forma correcta el servicio de emisión de sellos digitales de tiempo.
15. La reventa, copias y servicios no autorizadas de los sellos digitales de tiempo de Legalex GS por o aún 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 los sellos digitales de tiempo de Legalex GS se atendrán a los términos y condiciones de la TSA las cuales estipulan:

1. Verificar que el token recibido por parte del servicio de emisión 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 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 al servicio de emisión sellos digitales de tiempo y/o a los sellos digitales de tiempo emitidos o proveídos.

Responsabilidades

Responsabilidades del PSC.

Las responsabilidades principales que tiene Legalex GS como una TSA 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 correspondientes 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 los sellos digitales de tiempo que expida Legalex GS son válidos y mantienen la estructura que se declara en este documento.
4. El token o identificador de sello de tiempo 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. Los sellos digitales de tiempo emitidos por la TSA de Legalex GS, deben usarse únicamente en los casos establecidos en la declaración de prácticas de sellos digitales de tiempo en su apartado de aplicabilidad.
8. Estas responsabilidades no afectan una implicación directa en el cobro del servicio de emisión de sellos digitales de tiempo.
9. EL detalle de todas las responsabilidades del PSC se integra 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 los sellos digitales de tiempo deben acatar las siguientes responsabilidades:

1. Resguardar los archivos que se dan como efecto de cada SDT, administrar sus propias copias de seguridad de los archivos que sellen y los archivos provenientes del servicio.
2. Resguardar las claves empleadas para tener acceso al servicio de SDT.
3. 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.
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 sello digital de tiempo solo sea usado para fines y propósitos comerciales ya autorizados como son, asuntos del orden comercial conforme al Código de comercio en el artículo 101 numeral IV emitido por la Cámara de diputados del H. Congreso de la Unión y lo presentado en este documento.
6. Cuidar el uso que se le dé al dispositivo o medio electrónico donde guarde sus credenciales o claves para el acceso de SDT, así como otros documentos o archivos expedidos por el personal que le entregue el contrato de prestación del servicio de SDT.

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 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 siguientes situaciones:

1. El uso inadecuado o no autorizado de un sello digital de tiempo solicitados por algún suscriptor o cliente.
2. Sellos digitales de tiempo emitidos o proveídos por terceras personas que tengan acceso a las credenciales de algún suscriptor.
3. Sellos digitales de tiempo emitidos o proveídos con información fraudulenta o falsa, sin importar que el cliente o suscriptor del servicio lo tenga en su resguardo.
4. Sellos digitales de tiempo 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, TSA o al cliente/suscriptor, ambos quedarán deslindados de responsabilidades.
7. Que el servicio de transferencia segura de la escala de tiempo UTC del CENAM falle.

8. 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, TSA o al cliente/suscriptor, ambos quedarán deslindados de responsabilidades.

Restricciones de uso de los Sellos digitales de Tiempo

Los sellos digitales de tiempo emitidos por la TSA del 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 un sello digital de tiempo.

El uso de los sellos digitales de tiempo queda limitado por sus políticas de uso y su aplicabilidad como se marcan en las Políticas de sellos digitales de tiempo 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 3628.

Responsabilidades Económicas

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

1. 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 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 sello digital de tiempo.
    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 SDT, 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.

Resaltando:

1. Cualquier limitación en su uso.
2. Obligaciones del suscriptor.
3. Información sobre cómo validar el SDT de un archivo o documento.
4. Cualquier limitación de responsabilidad, incluyendo los efectos / usos para los que la AC acepta (o excluye) responsabilidad.
5. Los procedimientos de reclamo y solución de controversias.

Políticas de Sellado de tiempo

Identificación

El identificador de objeto (X.208) utiliza la notación ASN.1 de la política del sellado de tiempo. 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 el sello digital de tiempo o en su defecto los certificados que se utilizarán para el proceso de emisión de sellos digitales de tiempo. El tipo de certificado utilizado en el proceso de emisión del sello digital 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 (CAdES-T)*" y 4.4.2 "*ES with complete validation Data References (CAdES-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

Todos los servicios de emisión de sellos digitales de tiempo que utilicen a la Autoridad de Sellado de tiempo llevarán un identificador, la causa es que la TSA utiliza y utilizará el identificador de las políticas de sellos digitales de tiempo en el token o identificador del sello de tiempo, como se explica en el tema "*Identificación*" de este documento.

Legalex GS reclamará la conformidad con el presente documento aplicado en las políticas de sellos digitales de tiempo, identificando el sello digital de tiempo que se emiten 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 identificada dentro del 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 de tener una relación jerárquica con el departamento que opera la TSA. Las auditorias deberán realizarse por un auditor independiente y competente, como se establece en la *RFC 3628, tema 5.4 Conformance,* inciso b.
3. Sí la TSA ha sido auditada o evaluada por una parte independiente.
4. La TSA demostrará que cumple con sus obligaciones tal y como se define en el título *Obligaciones de la TSA* de este mismo documento.
5. El PSC implementará los controles que cumplan con los requisitos de la Declaración de prácticas de Sellos digitales de tiempo.
6. Cuando exista la evaluación de conformidad con las políticas de sellos digitales de tiempo y los procesos auditados por parte de la TSA; 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.
7. 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".
8. 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 emitir sellos digitales de tiempo 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 TSA se verificará regularmente y cada vez que se realice un cambio importante en sus operaciones.

Aplicabilidad

Los sellos digitales de tiempo 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 SDT, 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 del Sello Digital de Tiempo.*

La declaración de prácticas de SDT va en cumplimiento con las Reglas generales a las que deberán sujetarse los PSC en su regla 118, que establece la Secretaria de Economía para ofrecer el servicio de emisión de sellos digitales de tiempo.

El Sello Digital de Tiempo que expedirá la ASDT 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 a los RFC 3628 y RFC 3161.

Organización

Legalex GS se encuentra acreditada como PSC por la Secretaría de Economía de los Estados Unidos Mexicanos y se encuentra habilitada como una Autoridad de Sellado de Tiempo (TSA) y como tal cumple con las siguientes clausulas:

1. Las políticas y procedimientos bajo los cuales opera la TSA no son discriminatorias.
2. Legalex GS, pondrá sus servicios como TSA 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 TSA.
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 calificados y cumplen con los requisitos expresados en las reglas generales a las que deben 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 TSA; sin embargo, en caso del cese de actividades de la TSA, 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 Sellado de Tiempo".

Consideraciones de seguridad

Al verificar los tokens o identificadores de sellos digitales de tiempo, es necesario, que el cliente que verifica la disponibilidad del SDT, se asegure de que el certificado de la TSU/TSA sea confiable y no se encuentre revocado. El certificado de SDT firmado por la Secretaría de Economía será de un periodo de 10 años.

Todas aquellas entidades que confíen en los sellos digitales de tiempo emitidos por Legalex GS, deben de asegurarse de que el certificado de firma de la TSU/TSA 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 SDT emitido o proveído por la TSA y su TSU, consultar el sitio https://www.legalexgs.com/Servicios/sellos/validar.jsp.

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

Anexos

Apéndice A

Acrónimos

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

Acrónimo	Significado
ASDT	Autoridad de Sellado de Tiempo.
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)
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)
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)
SDT	Sello Digital de Tiempo.
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)
TSA	Autoridad de sellado de tiempo.
TSU	Unidad de sellado de tiempo.
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

Trabajos Citados

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/

Cámara de Diputados del H. Congreso de la unión, Secretaría de Economía. (25 de Enero de 2017). *Código de comercio*. Obtenido de Cámara de diputados del H. Congreso de la unión: http://www.diputados.gob.mx/LeyesBiblio/pdf/3_250117.pdf

DigiCert. (01 de Enero de 2013). *SHA-2 Certificado Soluciones de DigiCert SHA-256 SSL*. Obtenido de DigiCert: https://www.digicert.com/es/certificados-ssl-con-sha2.htm

ETSI. (01 de Enero de 2017). *ETSI*. Obtenido de ETSI: http://www.etsi.org/

IEC - International Electrotechnical Commision. (22 de Junio de 2017). *International Electrotechnical Commision*. Obtenido de http://www.iec.ch/

IETF. (01 de Mayo de 2008). RFC 2508 - Cryptography Standards (PKCS). Hopkinton, Massachusetts, Estados Unidos.

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 for Standardization - ISO. (22 de Junio de 2017). *International Organization for Standardization*. Obtenido de https://www.iso.org/home.html

International Organization Standars. (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.

Legion of the Bouncy Castle Inc. (10 de Junio de 2013). *Welcom to Bouncy Castle*. Obtenido de bouncycastle.org: https://www.bouncycastle.org/

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 Standars and Technology. (25 de Mayo de 2001). Security requeriments for cryptographic modules. Gaithersb, Condado de Montgomery, Maryland. Obtenido de http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Pérez Porto, J., & Gardey, A. (01 de Enero de 2008). *Definición.de*. Obtenido de Definición.de: https://definicion.de/

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

RAE - Real Academia Española. (Junio de 2017). *Diccionario de la lengua española*. Obtenido de Real Academia Española: http://dle.rae.es/?w=diccionario

RedHat INC. (02 de Enero de 2017). *Cifrado de llave pública*. Obtenido de RedHad documentación, guía de seguridad: https://access.redhat.com/documentation/es-ES/Red_Hat_Enterprise_Linux/6/html/Security_Guide/apas02.html

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/

Seagate. (01 de Enero de 2012). *Tecnología estándar FIPS 140-2 y unidad de cifrado automático*. Obtenido de SEAGATE: http://www.seagate.com/la/es/tech-insights/fips-140-2-standard-and-self-encrypting-drive-technology-master-ti/

Secretaria 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

Seguridad Informática. (14 de Septiembre de 2007). *Qué es RSA*. Obtenido de Seguridad informática: https://seguinfo.wordpress.com/2007/09/14/%C2%BFque-es-rsa/

Via Firma developers. (01 de Enero de 2017). *Extensiones x.509 en certificados*. Obtenido de Developers vía firma: https://developers.viafirma.com/que-extensiones-de-archivo-de-certificados-de-estandar-x509-existen

Viafirma. (2017). Obtenido de https://www.viafirma.com/