Sectigo
Política y Declaración de prácticas de la TSA eIDAS

Sectigo (Europe) SL
Versión 1.1.0
Efectivo: 27 de Octubre de 2023
Rambla Catalunya, 86 3 1,
08008 Barcelona, España
ww.sectigo.com

Aviso de copyright

Copyright 2023 Sectigo. Reservados todos los derechos.

Ninguna parte de esta publicación puede ser reproducida, almacenada o introducida en un sistema de recuperación, o transmitida, en cualquier forma o por cualquier medio (electrónico, mecánico, fotocopiado, grabación u otro) sin el permiso previo por escrito de Sectigo. Las solicitudes de cualquier otro permiso para reproducir este documento de Sectigo (así como las solicitudes de copias de Sectigo) deben dirigirse a:

Sectigo (Europe) SL
Rambla Catalunya, 86 3 1,
08008 Barcelona, España

Contenido

INTRODUCCIÓN

Sectigo es un proveedor de servicios de confianza (TSP) que emite tokens de sellos de tiempo digitales confiables a entidades, incluidas empresas públicas y privadas e individuos, de acuerdo con esta política y declaración de prácticas de sellos de tiempo de Sectigo.

Sectigo cuenta con un servicio de sellado de tiempo cualificado que proporciona tokens de sello de tiempo cualificados de acuerdo con el reglamento de la UE 910/2014 del 23 de julio de 2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado único europeo, que deroga la directiva 1999/93 / EC de 13 de diciembre de 1999, comúnmente denominado eIDAS. Sectigo cumple con los requisitos establecidos en el artículo 42 del Reglamento (UE) 910/2014.

Esta Política y Declaración de Prácticas de Sellado de Tiempo (TSPPS) se aplica a los Servicios de Sellado de Tiempo Cualificados de eIDAS de Sectigo.

Este documento establece solo prácticas específicas adicionales de sellado de tiempo de acuerdo con eIDAS.

En su rol de TSP, Sectigo realiza funciones asociadas con operaciones de clave pública que incluyen recibir solicitudes, emitir, etc. para usuarios dentro de la Infraestructura de Clave Pública (PKI) de Sectigo.

1. Alcance

Este documento describe la política y la declaración de prácticas de sellado de tiempo, especificando las políticas y procesos generales para crear y emitir sellos de tiempo y los servicios adicionales asociados.

En este documento se especifican detalles técnicos y procesos específicos además de aquellos indicados en la CPS general de Sectigo según eIDAS.

Para la emisión de tokens de sellos de tiempo cualificados, Sectigo cumple con la norma ETSI EN 319 421 “Policy and Security requirements for Trust Service Providers issuing Time-Stamps”. Además, Sectigo también sigue la norma ETSI EN 319 422 “Time-stamp protocol and time-stamp token profiles” para la definición del perfil de sello de tiempo.

Este documento es solo uno de un conjunto de documentos relevantes para la prestación de Servicios de Sellado de Tiempo por Sectigo y que la lista de documentos contenidos en este documento son otros documentos que se mencionarán de vez en cuando.

Este documento, los acuerdos y políticas relacionados a los que se hace referencia en este documento están disponibles en *www.sectigo.com/legal*.

2. Referencias

Para efectos del presente documento, se aplican las normas referenciadas en la DPC según eIDAS y además los siguientes:

ETSI EN 319 421 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps

ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

Recommendation ITU-R TF.460-6 - Standard-frequency and time-signal emissions

RFC 1305 - Network Time Protocol

RFC 5816 – ESSCertIDv2 Update for RFC 3161

3. Definiciones y abreviaturas

3.1. Definiciones

A los efectos del presente documento, se aplican las definiciones dadas en la DPC según eIDAS y las siguientes:

Término	Definición
Hora universal coordinada	escala de tiempo basada en el segundo según se define en la Recomendación UIT-R TF.460-6
Protocolo de tiempo de red	es un protocolo de red para la sincronización del reloj entre sistemas informáticos a través de redes de datos de latencia variable conmutadas por paquetes.
Sello de tiempo	Datos en forma electrónica que vinculan otros datos electrónicos a un momento particular, estableciendo evidencia de que estos datos existían en ese momento.
Autoridad de Sellado de Tiempo (TSA)	TSP que proporciona servicios de sellado de tiempo utilizando una o más unidades de sellado de tiempo
Servicio de sellado de tiempo	Servicio de confianza para la emisión de sellos de tiempo
Servicio de confianza	Servicio electrónico que mejora la confianza y la seguridad en las transacciones electrónicas.
Declaración de prácticas y políticas de la TSA	declaración de la política y las prácticas que emplea una TSA para emitir sellos de tiempo
Unidad de sellado de tiempo (TSU)	conjunto de hardware y software que se gestiona como una unidad y tiene una única clave de firma de sello de tiempo activa a la vez
UTC (k)	Escala de tiempo realizada por el laboratorio “k” y mantenida en estrecha concordancia con UTC, con el objetivo de alcanzar + - 100 ns

3.2. Abreviaturas

A los efectos del presente documento, se aplican las siglas que figuran en la DPC según eIDAS y las siguientes:

Acrónimo	**Nombre completo**
NTP	Protocolo de tiempo de red
TSA	Autoridad de Sellado de Tiempo
TSU	Unidad de sello de tiempo
TSPPS	Declaración de prácticas y políticas de sellos de tiempo
UTC	Hora universal coordinada

4. Conceptos generales

4.1. Conceptos de requisitos de la política

Esta TSPPS considera la ETSI EN 319 401 como una referencia para los requisitos de política comunes a todas las clases de servicios de proveedores de servicios de confianza.

Estos requisitos se basan en el uso de criptografía de clave pública, certificados de clave pública y fuentes de tiempo confiables.

Se espera que el suscriptor y los terceros de confianza consulten esta TSPPS para obtener más detalles sobre cómo esta política de sello de tiempo es implementada por la TSA (por ejemplo, los protocolos utilizados para brindar este servicio).

4.2. Servicios de sellado de tiempo

La prestación de servicios de sellado de tiempo se desglosa en este documento en los siguientes servicios a los efectos de clasificar los requisitos:

- Provisión de sellos de tiempo: este componente de servicio genera sellos de tiempo.
- Gestión de sellado de tiempo: este componente de servicio supervisa y controla el funcionamiento de los servicios de sellado de tiempo para garantizar que el servicio prestado sea el especificado por la TSA. Este componente de servicio tiene la responsabilidad de la instalación y desinstalación del servicio de provisión de sellado de tiempo.

4.3. Autoridad de Sellado de Tiempo (TSA)

Un Proveedor de Servicios de Confianza (TSP) que proporciona servicios de sellado de tiempo al público se denomina Autoridad de Sellado de Tiempo (TSA). La TSA tiene la responsabilidad general de la prestación de los servicios de sellado de tiempo identificados en la cláusula 4.2. La TSA tiene la responsabilidad de la operación de una o más TSU que crea y firma en nombre de la TSA.

La TSA puede hacer uso de otras partes para proporcionar parte de los servicios de sellado de tiempo. Sin embargo, la TSA siempre mantiene la responsabilidad general y garantiza que se cumplan los requisitos de la política identificados en este TSPPS.

Las CA emiten certificados a las Unidades de Sellado de Tiempo de la TSA. Estos certificados permiten a las partes que confían identificar la TSA.

Este servicio está disponible en *http://timestamp.sectigo.com/qualified*

Los relojes TSU son supervisados localmente por los servidores de tiempo de referencia. Estos servidores son autónomos y se benefician de un procedimiento de sincronización con las referencias UTC (k).

4.4. Suscriptor

El Suscriptor es la persona física o jurídica que posee el sello de tiempo producido por la TSA. El Suscriptor es la persona física o jurídica que acepta los términos y condiciones definidos en el Acuerdo de Suscriptor.

4.5. Política de sello de tiempo y declaración de prácticas de la TSA

Esta cláusula explica los roles relativos de la política de sellos de tiempo y la declaración de prácticas de la TSA. No impone ninguna restricción sobre la forma de una política de sello de tiempo o una especificación de declaración de prácticas.

Una política de sello de tiempo es una forma de Política de servicio de confianza como se especifica en ETSI EN 319 401 aplicable a los proveedores de servicios de confianza que emiten sellos de tiempo.

La Declaración de prácticas de la TSA es una forma de Declaración de prácticas de servicios de confianza según se especifica en ETSI EN 319 401 aplicable a los proveedores de servicios de confianza que emiten sellos de tiempo.

Este documento especifica la política de sello de tiempo y la declaración de prácticas para Sectigo TSA.

5. Políticas de sello de tiempo

5.1. General

Este documento define un conjunto de reglas a las que se adhiere Sectigo al emitir sellos de tiempo, respaldadas por certificados de clave pública, con una precisión de un (1) segundo o mejor frente a UTC.

5.2. Política e Identificación

Este documento es la Declaración de Prácticas y Políticas de Sellado de Tiempo cualificada por Sectigo eIDAS.

Define los compromisos de la TSA en materia de seguridad y organización de los procesos para la emisión y gestión de sellos de tiempo emitidos por estas TSAs.

El identificador de la política de certificados en los certificados de la TSA especificados en el presente documento es: 1.3.6.1.4.1.6449.1.2.1.9

Al incluir este identificador de objeto itu-t (0) identified-organization (4) etsi (0) time stamp-policy (2023) policy-identifiers (1) best-practices-ts-policy (1) en un token de sello de tiempo, Sectigo afirma que cumple con esta política de sello de tiempo.

Cuando Sectigo declara un sello de tiempo cualificado según el reglamento de la UE 910/2014 (eIDAS), el certificado para la validación de la firma se emite bajo la política de certificados declarada en ETSI EN 319 411-2, que también incorpora los requisitos ETSI EN 319411-1.

5.3. Comunidad de usuarios y aplicabilidad

Este documento tiene como objetivo cumplir con los requisitos de los sellos de tiempo para una validez a largo plazo, pero generalmente se aplica a cualquier uso que tenga un requisito de calidad equivalente.

Este documento se puede utilizar para servicios públicos de sellado de tiempo o servicios de sellado de tiempo utilizados dentro de una comunidad cerrada.

6. Políticas y prácticas

6.1. Evaluación de riesgos

Al igual que la mayoría de las organizaciones que operan en un entorno cada vez más dependiente de la información y la tecnología, Sectigo y sus subsidiarias corporativas (denominadas colectivamente "Sectigo") a menudo están expuestas a posibles amenazas a la seguridad de la información que, si resultan en un incidente, tienen la capacidad para causar pérdidas financieras directas a Sectigo, interrupciones operativas y daños a la reputación de la empresa. Sectigo considera su información como un activo de gran valor y, como resultado, nuestros sistemas de procesamiento e información son fundamentales para nuestro negocio y deben protegerse adecuadamente.

La información puede existir en una variedad de formas, ya sean electrónicas, en papel y otros tipos de medios, y lleva consigo detalles importantes y, en ocasiones, críticos relacionados con las actividades diarias y estratégicas de los negocios de Sectigo y de nuestros clientes y socios comerciales. La pérdida, corrupción o robo de información o sistemas comerciales de soporte podrían tener un impacto grave en la integridad de las actividades comerciales y la reputación de Sectigo.

Este Marco de Gestión de Riesgos se define para todos los activos y actividades relacionados con los procesos comerciales de Sectigo.

El enfoque de Sectigo para la gestión de riesgos consta de dos áreas:

- Evaluación de riesgos: una evaluación de las amenazas, los impactos y las vulnerabilidades de los activos y la probabilidad de que ocurran.
- Tratamiento de riesgos: Proceso de selección e implementación de controles de seguridad con el fin de reducir los riesgos identificados en la evaluación de riesgos a un nivel aceptable.

Sectigo realiza una evaluación de riesgos completa en toda la organización anualmente.

6.2. Declaración de prácticas de servicio de confianza

Sectigo garantizará la calidad, el rendimiento y el funcionamiento del servicio de sellado de tiempo mediante la implementación de diversas políticas y controles de seguridad.

Las políticas y controles de seguridad son revisados periódicamente por un organismo independiente, mientras que personal capacitado y confiable verifica el cumplimiento de los controles de seguridad con las políticas.

Adicionalmente, para el cumplimiento de ETSI EN 319 421 se han implementado las siguientes medidas

6.2.1. Formato de sello de tiempo

Los tokens de sello de tiempo emitidos por Sectigo cumplen con RFC 3161/5816 y ETSI EN 319 422. El servicio emite sellos de tiempo RSA 4096 que utilizan el algoritmo hash SHA384.

Consulte el Anexo B para obtener información adicional.

6.2.2. Precisión del tiempo

Como fuente confiable de tiempo, Sectigo tiene un pequeño subconjunto de nuestras máquinas que se comunican con las fuentes del Estrato 1 y también con el Estrato 2 o 3 como referencia.

El servicio de sellado de tiempo utiliza esta señal de tiempo junto con un monitor de tiempo NTP para monitorear el tiempo, el desplazamiento y la deriva del tiempo desde un conjunto de servidores NTP de laboratorios UTC (k). Con esa configuración, el servicio de sello de tiempo alcanza una precisión de la hora muy por debajo de +/- 1 s con respecto a UTC.

Todos los servidores que usa la TSA de Sectigo ejecutan ntpd que a su vez se comunican con varios servidores de tiempo redundantes para mantener el tiempo sincronizado.

Sectigo utiliza fuentes NTP de proveedores de tiempo nacionales, universidades y proyectos específicos.

6.2.3. Obligaciones del suscriptor

Consulte el acuerdo de suscripción para obtener información adicional.

6.2.4. Obligaciones de los terceros de confianza

Los terceros de confianza utilizan los servicios PKI en relación con varios certificados o sellos de tiempo de Sectigo para los fines previstos y pueden confiar razonablemente en dichos certificados o sellos de tiempo.

Los terceros de confianza están sujetos a las estipulaciones del acuerdo establecidos entre las partes.

6.2.5. Verificación del sello de tiempo

La verificación del sello de tiempo incluye lo siguiente

6.2.5.1. Verificación del emisor del sello de tiempo

Una TSA que utiliza certificados electrónicos adecuados emite el sello de tiempo. Las claves públicas de los certificados utilizados, incluidos los certificados TSU y CA, se publican para permitir una verificación de que la TSA ha firmado correctamente el sello de tiempo.

6.2.5.2. Verificación del estado de revocación del sello de tiempo

Un servicio de respuesta OCSP está disponible para verificar el estado de revocación de los certificados usados en el sello de tiempo.

6.2.6. Cumplimiento de la ley aplicable

Este TSPPS está sujeto a las leyes, reglas, regulaciones, ordenanzas, decretos y órdenes nacionales, estatales, locales y extranjeras aplicables, incluidas, entre otras, restricciones sobre la exportación o importación de software, hardware o información técnica. Sectigo cumple con todas las leyes, reglas, regulaciones, ordenanzas, decretos y órdenes aplicables cuando brinda servicios de conformidad con este TSPPS.

Específicamente, Sectigo TSA cumple con:

- Reglamento eIDAS
- ETSI EN 319401, 319 421 y 319 422
- RFC 3161/5816

6.2.7. Servicio disponible

Sectigo ha implementado las siguientes medidas para asegurar la disponibilidad del servicio:

- Configuración redundante de sistemas de TI, incluida la infraestructura de HSM, para evitar puntos únicos de falla
- Conexiones a Internet redundantes de alta velocidad para evitar la pérdida de servicio
- Uso de fuentes de alimentación ininterrumpidas.

Sectigo apunta a brindar un 99,9% de disponibilidad de servicio al año.

6.3. Términos y condiciones

Sectigo publica este TSPPS, los términos y condiciones, el Acuerdo de terceras partes de confianza y los Acuerdos del suscriptor en el Repositorio.

La información sobre las limitaciones del servicio, los términos y condiciones se pueden consultar en el documento de términos de uso.

6.4. Política de seguridad de la información

Sectigo ha implementado una política de seguridad de la información que todos los empleados deben cumplir. La política de seguridad de la información se revisa periódicamente y cuando ocurren cambios significativos.

6.5. Obligaciones de la TSA

6.5.1. General

La TSA es responsable de:

- El cumplimiento de este TSPPS y sus políticas y procedimientos internos o publicados.
- El cumplimiento de las leyes y regulaciones aplicables.
- Proporcionar infraestructura y servicios de certificación, que incluyen, entre otros, el establecimiento y funcionamiento del Repositorio de Sectigo y el sitio web para el funcionamiento de los servicios de PKI.
- Proporcionar mecanismos de confianza, incluido un mecanismo de generación de claves, protección de claves y procedimientos de intercambio de secretos con respecto a su propia infraestructura.
- Proporcionar un aviso rápido en caso de que se comprometa su (s) clave (s) privada (s).
- El cumplimiento de los sellos de tiempo
- El cumplimiento de todos los diferentes componentes de la TSA y los controles relacionados con los principios de seguridad.
- Brindar soporte a los suscriptores y a los terceros de confianza como se describe en esta TSPPS.
- Poner a disposición de las partes solicitantes una copia de este TSPPS y las políticas aplicables.

6.5.2. Obligaciones de la TSA hacia los suscriptores

El presente documento no impone obligaciones específicas al suscriptor más allá de los requisitos específicos de la TSA establecidos en los términos y condiciones de la TSA.

6.6. Información para los terceros de confianza

Las obligaciones de las partes que confían están cubiertas en el acuerdo establecido entre ambas partes. Además, estos terceros de confianza deberán hacer lo siguiente:

- verificar que el sello de tiempo se haya firmado correctamente y que la clave privada utilizada para firmar el sello de tiempo no se haya visto comprometida hasta el momento de la verificación;
- tener en cuenta cualquier limitación en el uso del sello de tiempo indicado por la política de sello de tiempo
- Tener en cuenta cualquier otra precaución prescrita en acuerdos o en cualquier otro documento.

7. Gestión y operación de la TSA

7.1. Introducción

Sectigo ha implementado políticas de seguridad de la información y procedimientos operativos para mantener la seguridad del servicio.

Sectigo puede cobrar tarifas de suscriptor por algunos de los servicios que ofrece.

Sectigo se reserva el derecho de modificar dichos cargos.

7.2. Organización interna

Para el correcto funcionamiento del servicio de sellado de tiempo, Sectigo mantiene documentación no divulgada que especifica todos los controles operativos relacionados con la seguridad del personal, controles de acceso, evaluación de riesgos, etc. Estos documentos internos son utilizados por organismos independientes para confirmar el cumplimiento del servicio con la norma ETSI EN 319421.

- Entidad legal: La TSA es proporcionada por Sectigo.
- La gestión de la seguridad de la información y la gestión de la calidad del servicio se realiza dentro del concepto de seguridad del servicio.
- Sectigo opera su TSU desde un centro de datos, que proporciona la infraestructura básica (acceso a Internet, electricidad, seguridad física, etc.) del servicio de confianza.

7.2.1. Persona de contacto

Se puede contactar a la autoridad de políticas de Sectigo en la siguiente dirección:

Autoridad de políticas de Sectigo
3.er piso, edificio 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, Reino Unido
Tel: +44 (0) 161 874 7070
URL: *https://www.sectigo.com*
Correo electrónico: *legalnotices@sectigo.com*

7.3. Personal de Seguridad

El acceso a las partes seguras de las instalaciones de Sectigo está limitado mediante controles de acceso físicos y lógicos y solo pueden acceder las personas debidamente autorizadas que desempeñan funciones de confianza para las que están debidamente cualificadas y para las que han sido nombradas por la dirección.

Sectigo requiere que todo el personal que desempeña funciones de confianza esté debidamente capacitado y tenga la experiencia adecuada antes de que se le permita adoptar esas funciones.

7.3.1. Requisitos de calificaciones, experiencia y autorización

De acuerdo con este TSPPS, Sectigo sigue prácticas de gestión y personal que brindan una garantía razonable de la confiabilidad y competencia de sus empleados y del desempeño satisfactorio de sus funciones.

7.3.2. Procedimientos de verificación de antecedentes

Todo el personal de confianza tiene verificaciones de antecedentes antes de que se otorgue acceso a los sistemas de Sectigo. Estas verificaciones pueden incluir, entre otras, la verificación de la identidad de la persona mediante una identificación con foto emitida por el gobierno, historial crediticio, historial de empleo, educación, referencias de carácter, número de seguro social, antecedentes penales y una referencia cruzada de la Cámara de Empresas para directores.

7.3.3. Requisitos de formación

Sectigo proporciona una formación adecuada a todo el personal antes de que asuman un puesto de confianza en caso de que no tengan ya el conjunto completo de habilidades necesarias para ese puesto. La formación del personal se lleva a cabo mediante un proceso de tutoría en el que participan miembros de alto nivel del equipo al que están adscritos.

7.3.4. Frecuencia y requisitos de re-formación

El personal en funciones de confianza tiene capacitación adicional cuando los cambios en los estándares de la industria o los cambios en las operaciones de Sectigo lo requieren. Sectigo ofrece formación de repaso y actualizaciones informativas suficientes para garantizar que el personal de confianza conserve el grado de experiencia necesario.

7.3.5. Frecuencia y secuencia de rotación de trabajos

Sectigo asegura que cualquier cambio en el personal no afectará la efectividad operativa del servicio o la seguridad del sistema.

7.3.6. Sanciones por acciones no autorizadas

Cualquier personal que, a sabiendas o por negligencia, viole las políticas de seguridad de Sectigo, exceda el uso de su autoridad, use su autoridad fuera del alcance de su empleo o permita que el personal bajo su supervisión lo haga, puede estar sujeto a acciones disciplinarias que incluyen terminación del empleo. Si las acciones no autorizadas de cualquier persona revelan una falla o deficiencia en la capacitación, se empleará la formación suficiente para rectificar la deficiencia.

7.3.7. Requisitos del contratista independiente

Una vez que el contratista independiente completa el trabajo para el cual fue contratado, o se termina el empleo del contratista independiente, todos los derechos de acceso asignados a ese contratista se eliminan lo antes posible y dentro de las 24 horas posteriores al momento de la terminación.

7.3.8. Documentación suministrada al personal

La selección de la documentación suministrada al personal de Sectigo se basa en los roles que deben desempeñar. Dicha documentación puede incluir una copia de este TSPPS, el reglamento eIDAS y otra documentación técnica y operativa necesaria para mantener las operaciones de la TSA de Sectigo.

7.4. Gestión de activos

La gestión de los activos de Sectigo se basará en su clasificación en términos de su valor, requisitos legales, sensibilidad y criticidad para Sectigo. Las clasificaciones y los controles de protección asociados para los activos deben tener en cuenta las necesidades comerciales de compartir y restringir información y los impactos comerciales asociados con dichas necesidades.

Los activos se dividen en las siguientes categorías:

- Activos de información: información relacionada con los activos, mantenida en papel, bases de datos o archivos de datos. Esto incluye, entre otros, documentación del sistema, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, archivos de respaldo, información archivada.
- Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades del sistema.
- Activos físicos: equipos informáticos, medios extraíbles, equipos de comunicaciones (enrutadores, conmutadores, etc.) y otros equipos técnicos.
- Servicios - Servicios de comunicación / Internet.
- Personal: todos los empleados, contratistas y terceros de Sectigo.

7.5. Control de acceso

Las diferentes capas de seguridad con respecto al acceso físico y al acceso lógico garantizan un funcionamiento seguro del servicio de sellado de tiempo.

El acceso a la información de Sectigo, las instalaciones de procesamiento de información y los procesos comerciales deben controlarse en función de los requisitos comerciales y de seguridad. Esta política considerará:

- Responsabilidades y gestión del acceso de los usuarios.
- Gestión de acceso a la red.
- Gestión de acceso al sistema operativo, aplicaciones y bases de datos.

7.6. Controles criptográficos

Sectigo utiliza varias claves privadas para cumplir con su servicio. Se utiliza un par de claves para emitir los certificados de sello de tiempo que se utilizan dentro de las TSU.

Todas las claves privadas se almacenan en un módulo de seguridad de hardware (HSM) certificado según FIPS 140-2 Nivel 3 o QSCD.

7.6.1. Generación de pares de claves TSU

Para los pares de claves de TSU creados bajo este TSPPS, Sectigo prepara y sigue un script de generación de claves.

Las claves de Sectigo se generan y se guardan en módulos de seguridad de hardware (HSM) que cumplen, como mínimo, con FIPS 140-2 nivel 3, o que están listados como QSCD.

Todas las operaciones clave se realizan dentro de la seguridad del HSM. Todas las claves que se exportan desde el HSM se cifran con un algoritmo de cifrado adecuado con la clave de cifrado generada por el HSM.

El acceso a estas claves está restringido al personal autorizado y de confianza de Sectigo. Los datos clave deben almacenarse de forma segura en todo momento a menos que sean atendidos por personal autorizado de Sectigo.

El acceso al software de operación criptográfica en el HSM se controla, como mínimo, mediante el uso de tarjetas inteligentes y PIN para varias personas, que deben ingresarse / presentarse antes de que se pueda realizar cualquier operación clave. El acceso a las tarjetas inteligentes y los PIN está restringido a los oficiales autorizados de Sectigo bajo control de varias personas (la configuración de Sectigo requiere que estén presentes N de las tarjetas M). Se registra el personal autorizado de Sectigo con acceso a tarjetas inteligentes y PIN.

Sectigo usa SHA384 en las respuestas de los sellos de tiempo.

Estas operaciones clave, por ejemplo, generación de claves, respaldo y recuperación que involucran un HSM, se realizan en una ceremonia clave. Todas las ceremonias clave se realizan en un área segura y controlada. Durante la ceremonia, al menos dos miembros del personal autorizado de Sectigo están presentes en todo momento.

No se permiten otras personas en el área segura durante las ceremonias clave para protegerse contra la pérdida de información por manipulación o supervisión. Toda la información "sensible" visible se mantiene al mínimo en todo momento durante las ceremonias clave.

Todas las ceremonias clave se realizan en una computadora con una instalación limpia verificada del sistema operativo que está aislado de todas las redes. El software de control de operaciones criptográficas será una instalación nueva y se verificará que funcione correctamente antes de su uso.

Todos los medios creados a partir de una ceremonia clave deben clasificarse y almacenarse de acuerdo con esta clasificación.

Todos los medios obsoletos de una ceremonia de claves deben eliminarse de manera segura, es decir, destrucción, al final de la ceremonia o en un período máximo de 1 día hábil. Todos los medios que no se eliminen por completo de inmediato deben destruirse parcialmente y almacenarse de forma segura hasta que se lleve a cabo la eliminación completa.

7.6.2. Protección de clave privada TSU

La infraestructura de Sectigo utiliza sistemas confiables. Un sistema confiable es el hardware, software y procedimientos que brindan una resistencia aceptable contra los riesgos de seguridad, brindan un nivel razonable de disponibilidad, confiabilidad y operación correcta, y hacen cumplir una política de seguridad.

7.6.2.1. Estándares y controles de módulos criptográficos

Sectigo genera y protege de forma segura su (s) propia (s) clave (s) privada (s), utilizando un sistema confiable certificado según FIPS 140-2 Nivel 3 o superior o listado como QSCD, y toma las precauciones necesarias para evitar el compromiso o el uso no autorizado de la misma.

La TSA garantiza la seguridad de estos módulos durante todo su ciclo de vida. En particular, la TSA implementa los procedimientos requeridos para:

- asegurar su integridad durante su transporte desde el proveedor
- Asegurar su integridad durante su almacenamiento antes de la ceremonia clave.
- Asegurar que las operaciones de activación de las claves de firma se lleven a cabo bajo el control de dos miembros del personal con roles de confianza.
- Asegurarse de que estén en un estado funcional adecuado.
- asegurándose de que las claves que contienen se destruyan después de ser retiradas.

7.6.2.2. Copia de seguridad de la clave privada

Las claves privadas de TSU se respaldan en consecuencia.

7.6.2.3. Almacenamiento de clave privada en módulo criptográfico

Las claves privadas se generan y almacenan dentro de los módulos de seguridad de hardware (HSM) de Sectigo, que han sido certificados con al menos FIPS 140-2 Nivel 3 o listados como QSCD.

7.6.3. Certificado de clave pública de la TSU

Sectigo garantiza la integridad y autenticidad de las claves (públicas) de verificación de firmas de TSU de la siguiente manera:

- Las claves (públicas) de verificación de firma de TSU están disponibles para las partes que confían en certificados disponibles públicamente. Los certificados se pueden encontrar en *crt.sh | Sectigo Qualified Time Stamping Signer*
- La TSU no emite un sello de tiempo antes de que su certificado de verificación de firma (clave pública) se cargue en la TSU o en su dispositivo criptográfico. Al obtener un certificado de verificación de firma (clave pública), Sectigo verifica que este certificado se haya firmado correctamente (incluida la verificación de la cadena de certificados ante su autoridad de certificación de confianza).

7.6.4. Cambio de claves de la TSU

El período de validez del certificado de TSU no será mayor que el período de tiempo en el que el algoritmo elegido y la longitud de la clave se reconozcan como adecuados para su propósito.

Una vez al año o cuando se producen cambios significativos, la Autoridad de Políticas de Sectigo verifica los algoritmos criptográficos utilizados dentro de la TSU con los algoritmos reconocidos como adecuados.

7.6.5. Gestión del ciclo de vida de la firma de hardware criptográfico

Todo el hardware criptográfico se inspeccionará durante el proceso de puesta en servicio para garantizar la conformidad con el suministro y que no se encuentre evidencia de alteración ni mientras esté almacenado.

La instalación, activación y duplicación de las claves de firma de TSU en hardware criptográfico debe ser realizada solo por personal en roles confiables usando al menos control dual en un ambiente físicamente seguro.

Las claves de firma privadas de TSU almacenadas en el módulo criptográfico de TSU se borrarán al retirar el dispositivo de una manera que sea prácticamente imposible recuperarlas.

7.6.6. Fin del ciclo de vida de la clave TSU

La validez de todas las claves privadas utilizadas nunca excede la validez de los certificados emitidos con esas claves privadas. Sectigo emitirá un nuevo certificado TSU con una nueva clave privada al menos cada 15 meses.

Después de la expiración de las claves privadas, las claves privadas dentro del hardware criptográfico se destruyen de tal manera que las claves privadas no se pueden recuperar ni utilizar más.

7.7. Sellado de tiempo

7.7.1. Emisión de sellos de tiempo

El Servicio de sellado de tiempo cualificado de Sectigo emite sellos de tiempo cualificados que se ajustan al perfil de sello de tiempo definido en ETSI EN 319 422.

Estos sellos de tiempo se emiten de forma segura e incluyen la hora correcta.

Los valores de tiempo que utiliza la TSU en el sello de tiempo deberán ser rastreables hasta al menos uno de los valores de tiempo real distribuidos por un laboratorio UTC(k). Consulte la cláusula 7.7.2.

El sello de tiempo se firma mediante una clave generada exclusivamente para este fin.

La TSA de Sectigo rechaza cualquier intento de emitir sellos de tiempo firmados por una clave privada que corresponda a un certificado TSU que haya expirado simplemente reconfigurando periódicamente nuestra TSA para usar un certificado y una clave recién emitidos (y por lo tanto ya no usar el certificado anterior y la clave).

7.7.2. Sincronización de reloj

La TSA de Sectigo está conectada a algunos laboratorios UTC (k) como su fuente de tiempo principal. Estos incluyen laboratorios de todo el mundo, como NIST (EE. UU.), NICT (JP), BEV (AT) y AOS (PL). Sectigo está incluyendo más puntos finales NTP de estos laboratorios UTC (k), y de otras fuentes de vez en cuando, para obtener una precisión mejor de la hora.

La TSA garantiza que su reloj está sincronizado con la hora UTC durante todo el NTP con una precisión declarada de un segundo.

Más particularmente:

1. la calibración de cada reloj TSU se mantiene de tal manera que los relojes no pueden desviarse más allá de la precisión declarada;

2. los relojes de las TSU están protegidos de amenazas relacionadas con su entorno, que podrían dar lugar a una desincronización con la hora UTC mayor que la precisión declarada;

3. La TSA garantiza que se detectará la desviación del reloj interno de una TSU más allá de la precisión declarada.

4. si se detecta que el reloj de una TSU no está dentro de la precisión declarada, los sellos de tiempo ya no se generan;

5. La TSA garantiza que la sincronización del reloj se mantiene cuando se programa el intercalado de un segundo (leap second), según lo notificado por el organismo correspondiente. El cambio para tener en cuenta este segundo (leap second) se realiza

durante el último minuto del día en el que está programado este segundo. Se hace un registro de la hora exacta (según la precisión declarada) cuando se realiza este cambio.

7.8. Seguridad física y ambiental

Todos los sitios operan bajo una política de seguridad diseñada para brindar una garantía razonable de detección, disuasión y prevención del acceso lógico o físico no autorizado a las instalaciones relacionadas con la TSA.

7.8.1. Ubicación y construcción

Sectigo opera en todo el mundo, con operaciones separadas, investigación y desarrollo y sitios de operación de servidores. Las barreras físicas se utilizan para segregar áreas seguras dentro de los edificios y están construidas para extenderse desde el piso real al techo real para evitar la entrada no autorizada. Las paredes externas son de construcción sólida.

7.8.2. Acceso físico

Existen sistemas de acceso con tarjeta para controlar y monitorizar el acceso a todas las áreas de la instalación. El acceso a las máquinas físicas de Sectigo dentro de la instalación segura está protegido con armarios cerrados con llave y controles de acceso lógicos. Los perímetros de seguridad están claramente definidos para todas las ubicaciones de Sectigo. Todas las entradas y salidas de Sectigo están aseguradas o monitorizadas por personal de seguridad, personal de recepción o sistemas de monitorización/control.

Cualquier persona no autorizada estará acompañada por una persona autorizada mientras se encuentre en el área segura. Se registra cada entrada y salida hacia/desde el área físicamente segura.

7.8.3. Energía y aire acondicionado

Las instalaciones seguras de Sectigo tienen una fuente de alimentación primaria y secundaria y garantizan un acceso continuo e ininterrumpido a la energía eléctrica. Los sistemas de calefacción / ventilación de aire se utilizan para evitar el sobrecalentamiento y mantener un nivel de humedad adecuado.

7.8.4. Exposiciones al agua

Sectigo ha realizado esfuerzos razonables para garantizar que sus instalaciones seguras estén protegidas de inundaciones y daños por agua. Sectigo tiene personal ubicado en el lugar para reducir el alcance de los daños causados por una inundación y cualquier exposición posterior al agua.

7.8.5. Prevención y protección contra incendios

Sectigo ha realizado esfuerzos razonables para garantizar que sus instalaciones seguras estén protegidas del daño por fuego y humo (la protección contra incendios se realiza de acuerdo con

las regulaciones locales contra incendios). El equipo de TI está ubicado para reducir el riesgo de daños o pérdidas por incendio. El nivel de protección contra incendios refleja la importancia del equipo.

7.8.6. Almacén de datos

Entre otras formas, Sectigo protege los medios almacenándolos lejos de peligros de fuego / agua conocidos u obvios. Los medios también se respaldan en el CPD y fuera del CPD.

7.8.7. Depósito de basura

Sectigo elimina los residuos de acuerdo con las mejores prácticas de la industria. Sectigo cuenta con procedimientos para desechar todo tipo de medios, incluidos, entre otros, documentos en papel, hardware, dispositivos dañados y dispositivos ópticos de solo lectura. Estos procedimientos se aplican a todos los niveles de clasificación de la información, y el método de eliminación depende de la clasificación.

7.8.8. Copia de seguridad fuera del CPD

Sectigo hace una copia de seguridad de gran parte de su información en una ubicación segura fuera del CPD que está lo suficientemente distante para escapar de los daños de un desastre en la ubicación principal. El equipo de infraestructura, teniendo en cuenta los requisitos de criticidad y seguridad de la información, determina la frecuencia, retención y extensión de la copia de seguridad.

Copia de seguridad de:

- El software crítico de la TSA se realiza semanalmente y se almacena fuera del CPD.
- La información empresarial crítica se realiza a diario y se almacena fuera del CPD. El acceso a los servidores / medios de respaldo está restringido únicamente al personal autorizado.
- Los medios de comunicación se prueban periódicamente a través de la restauración para garantizar que se pueda confiar en ellos en caso de un desastre.

Los servidores / medios de respaldo están debidamente etiquetados de acuerdo con la confidencialidad de la información.

7.9. Seguridad de la operación

Sectigo emplea políticas y procedimientos aprobados para garantizar que toda la información y las instalaciones de procesamiento de información se operen de manera coherente, sin comprometer la seguridad de las operaciones o los servicios.

Este TSPPS considerará los siguientes aspectos:

- Procedimientos operativos y responsabilidades.

- Segregación de deberes/tareas.
- Gestión de capacidad.
- Separación de entornos operativos, de prueba y de desarrollo
- Control de software operativo
- Seguridad de la documentación del sistema.
- Medios físicos en tránsito.
- Información disponible públicamente.
- Consideración de auditoría de sistemas de información.

7.9.1. Procedimientos operativos y responsabilidades

- Los procedimientos operativos documentados deben planificarse, desarrollarse, autorizarse, documentarse y ponerse a disposición de todos los usuarios que los necesiten.

- Se deben preparar procedimientos documentados para las actividades del sistema asociadas con el procesamiento de información y las instalaciones de comunicación, por ejemplo, respaldo, mantenimiento de equipos, manejo de medios, clasificación de medios, control de acceso, seguridad física, etc.

- Los procedimientos operativos se tratarán como documentos formales con todos los cambios autorizados por la gerencia.

- Los procedimientos operativos se documentarán en un manual de operaciones. El manual de operaciones debe contener los siguientes temas:
    - Descripción general detallada de la arquitectura de todos los sistemas y aplicaciones
    - Descripción general de todas las interfaces;
    - Responsabilidades y suplentes normativas para tareas administrativas;
    - Proceso de gestión de cambios;
    - Gestión de la configuración;
    - Gestión de vulnerabilidades / parches;
    - Gestión de capacidad;
    - Copia de seguridad y recuperación;
    - Esquema de explotación forestal;
    - Proceso de escalación;
    - Gestión de usuarios.

- Las tareas críticas en las que el principio de los cuatro ojos puede ser necesario deben

identificarse, documentarse y aplicarse cuando se considere necesario. Los ejemplos típicos incluyen:
    - Mantenimiento remoto por terceros;
    - Active Directory altamente privilegiado, administración raíz;
    - Renovación de certificados raíz / intermedios.

- Todos los sistemas y aplicaciones deben configurarse de forma segura. Las políticas de seguridad de la información de Sectigo, junto con cualquier otra normativa interna, tienen prioridad sobre las mejores prácticas o los estándares de la industria.

7.9.2. Segregación de deberes/tareas

- Los deberes/tareas y responsabilidades del personal dentro de Sectigo se organizarán de manera que no sea posible que una sola persona autorice y lleve a cabo un cambio en los sistemas de producción, la infraestructura o los datos.

- El acceso físico a las instalaciones y equipos de fabricación de certificados estará limitado al personal autorizado y operado bajo al menos doble custodia.

- Las tareas de administración, registro y auditoría de cualquier sistema dentro de Sectigo se organizarán de manera que ninguna persona sea responsable de las tareas de administración y auditoría.

- El personal de desarrollo de sistemas no puede autorizar cambios de código en el entorno de producción ni aprobar la prueba de su propio código.

7.9.3. Gestión de capacidad

- Se debe documentar e implementar un proceso de gestión de la capacidad para garantizar la capacidad adecuada de los sistemas e infraestructura de TI. Este proceso de gestión de la capacidad se utilizará para:
    - Establecer límites para el rendimiento y la disponibilidad aceptables del servicio;
    - Monitorear el uso de recursos y enviar mensajes de advertencia al equipo de operaciones cuando se alcanzan los umbrales establecidos;
    - Hacer una proyección para los requerimientos de recursos futuros;
    - Asegurar la integridad y disponibilidad de los sistemas de información.

- El uso de los recursos debe ser monitoreado, ajustado y se harán proyecciones de los requisitos de capacidad futuros para asegurar el desempeño adecuado del sistema.

- Los requisitos de capacidad, como energía eléctrica, ancho de banda de la red, almacenamiento, se identificarán al agregar / modificar activos de procesamiento de información.

- Se aplicará el ajuste y la supervisión del sistema para garantizar y, cuando sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas.

- Los controles de detectives, como el análisis de tendencias, deben estar en su lugar para indicar problemas a su debido tiempo.

- Se prestará especial atención a los recursos que implican un tiempo de entrega o un costo elevados.

7.9.4. Separación de entornos operativos, de prueba y de desarrollo

- Los sistemas y aplicaciones de TI en entornos que no sean de producción deberán estar lógica y / o físicamente separados del entorno o entornos de producción. Esta regla también debería aplicarse a los entornos en la nube. Ejemplos de las medidas de separación son las siguientes:
    - Los sistemas de TI de entornos de producción y no producción deben colocarse en redes diferentes
    - Las aplicaciones de entornos de producción y no producción deben instalarse en diferentes sistemas de TI
    - Los datos de entornos de producción y no producción deben ser administrados por diferentes instancias de aplicación
    - Los derechos de acceso privilegiado a los entornos de producción y no producción deben ser diferentes
    - Los sistemas de TI de apoyo, como las copias de seguridad o los archivos compartidos, deben separarse entre entornos de producción y no productivos
    - Siempre que sea posible, se preferirá la separación física a la separación lógica para ofrecer una mayor seguridad.

- Los sistemas y aplicaciones de TI en entornos de no producción deben cumplir los mismos requisitos de seguridad de la información que los sistemas y aplicaciones de TI en entornos de producción si alojan o procesan datos de producción.

- Los sistemas y aplicaciones de TI en entornos de no producción deben cumplir los mismos requisitos de seguridad de la información que los sistemas y aplicaciones de TI en entornos de producción si alojan o procesan datos personales.

7.9.5. Control de software operativo

- Solo las funcionalidades, los servicios y las aplicaciones necesarios para cumplir con los requisitos operativos y comerciales deben instalarse y ejecutarse en sistemas y aplicaciones de TI en entornos de producción.

- Se debe desarrollar, documentar e implementar un proceso formal para instalar aplicaciones y habilitar servicios en sistemas y aplicaciones de TI en entornos de

producción. El proceso debe incluir los siguientes temas:

- Definir cuándo es preferible realizar la instalación
- Definir cuándo es necesaria una aprobación formal y por quién
- Diferenciar entre aplicaciones temporales y permanentes
- Desinstalar aplicaciones temporales cuando ya no sean necesarias
- Reglas a seguir al resolver problemas urgentes
- Documentación de los servicios y aplicaciones que deben instalarse /habilitado en sistemas de TI en entornos de producción para identificar fácilmente aplicaciones y servicios no autorizados.

7.9.6. Seguridad de la documentación del sistema

- Cuando corresponda, la documentación del sistema se protegerá contra el acceso no autorizado.

- La documentación del sistema se almacenará de forma segura y estará disponible en caso de incidente / desastre.

7.9.7. Transferencia de medios físicos

- Los medios que contienen información se protegerán contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.

- Se utilizará transporte o mensajería confiable cuando se transporten medios que contengan información de Sectigo.

- Los medios se entregarán al mensajero / representante de terceros solo después de la identificación adecuada.

- El embalaje de los medios será suficiente para proteger el contenido de cualquier daño físico que pueda surgir durante el transporte.

- Se adoptarán controles adicionales durante el transporte de información sensible. Por ejemplo, contenedor cerrado, entrega por parte del personal de Sectigo, empaquetado, división de información en varias rutas de entrega diferentes.

7.9.8. Información disponible públicamente

- El software, los datos y otra información que requiera un alto nivel de integridad en un sistema disponible públicamente deberán estar protegidos por un mecanismo apropiado.

- Sectigo llevará a cabo comprobaciones periódicas para comprobar la integridad de la información disponible públicamente.

- Los procesos formales de aprobación deberán estar realizados antes de que la información

propiedad de Sectigo se ponga a disposición del público.

7.9.9. Consideraciones de auditoría de sistemas de información

Las auditorías de seguridad de TI en los sistemas de información deben planificarse y acordarse adecuadamente. Los siguientes temas, como mínimo, deben planificarse cuidadosamente:

- Derechos de acceso necesarios para realizar la auditoría (principio de privilegio mínimo);
- Alcance y pruebas a realizar;
- Hora del día en que se realizará la auditoría;
- Duración prevista de la auditoría.

7.10. Seguridad de la red

Sectigo desarrolla, implementa y mantiene un programa de seguridad integral diseñado para proteger sus redes. En este programa de seguridad, las protecciones generales para la red incluyen:

- Segmentar todos los sistemas PKI en redes o zonas según su relación funcional, lógica y física;
- Aplicar los mismos controles de seguridad a todos los sistemas ubicados en la misma zona con un sistema;
- Mantener los sistemas de CA raíz en una zona de alta seguridad y en un estado fuera de línea o sin conexión a otras redes;
- Implementar y configurar sistemas de soporte de seguridad que protejan los sistemas y las comunicaciones entre los sistemas dentro de las zonas seguras y las comunicaciones con los sistemas que no son PKI fuera de esas zonas;
- Configurar controles de límites de red (cortafuegos, conmutadores, enrutadores y puertas de enlace) con reglas que solo admitan los servicios, protocolos, puertos y comunicaciones que Sectigo ha identificado como necesarios para sus operaciones;
- Para todos los sistemas PKI, implementación de controles de detección y prevención para protegerse contra virus y software malicioso; y
- Cambiar las claves de autenticación y contraseñas para cualquier cuenta privilegiada o cuenta de servicio en cualquier sistema TSU siempre que se cambie o revoque la autorización de una persona para acceder administrativamente a esa cuenta en el sistema TSU.

7.11. Gestión de incidentes

Sectigo garantiza que se empleen procesos efectivos de gestión de incidentes en Sectigo Ltd. y sus subsidiarias corporativas (denominadas colectivamente "Sectigo") para tener:

- Una respuesta consistente a los incidentes que ocurren en los sistemas y aplicaciones de Sectigo.

- Incidencias detectadas, reportadas y registradas.
- Funciones y responsabilidades claras definidas en los procesos de prevención y respuesta a incidentes.
- Incidencias analizadas y lecciones aprendidas.

Un incidente es cualquier violación de la seguridad de la información; es decir, cualquier evento que comprometa la integridad, confidencialidad y / o disponibilidad de los sistemas, aplicaciones de Sectigo o la información contenida en estos. Un incidente también se define como cualquier incumplimiento de las políticas o requisitos legales de Sectigo.

Un proceso formal de presentación de informes de gestión de incidentes, junto con un procedimiento de escalamiento y respuesta a incidentes, permitirá gestionar el incidente y restablecer las operaciones normales de manera oportuna.

El proceso permitirá analizar el incidente para identificar las posibles causas y permitir la mejora de las debilidades en los procesos de Sectigo para evitar que vuelva a ocurrir.

7.12. Recolección de evidencias

Se cubren todos los tipos de eventos registrados indicados en la CPS según eIDAS, incluidos los siguientes:

- Generación de sellos de tiempo
- Todos los eventos relacionados con el ciclo de vida de las TSUs (gestión de claves, gestión de certificados, …)
- Apagado / reinicio de las TSUs
- Desincronización de los relojes de las TSUs

7.13. Gestión de la continuidad del negocio

Sectigo opera un sistema TSA completamente redundante. En caso de pérdida a corto o largo plazo de la ubicación de una oficina, se incrementarán las operaciones en otras oficinas.

La TSA de respaldo está disponible en caso de que la TSA principal deje de funcionar. Todo el equipo informático crítico de Sectigo está alojado en una instalación de coubicación administrada en un CPS, y todo el equipo informático crítico está duplicado dentro de la instalación. Las fuentes de alimentación y conectividad entrantes se duplican. El equipo duplicado está listo para asumir la función de proporcionar la implementación de la TSA y permite a Sectigo especificar un tiempo máximo de interrupción del sistema (en caso de falla crítica del sistema) de 1 hora.

Las operaciones de Sectigo se distribuyen en varios sitios en todo el mundo. Todos los sitios ofrecen instalaciones para administrar el ciclo de vida de un token de sello de tiempo.

Además de un sistema TSA completamente redundante, Sectigo mantiene disposiciones para la activación de una TSA de respaldo y un sitio secundario en caso de que el sitio principal sufra una pérdida total de sistemas. Este plan de recuperación ante desastres establece que Sectigo se esforzará por minimizar las interrupciones en sus operaciones de TSA.

En caso de compromiso con el funcionamiento de una TSU (p. ej., compromiso de la clave de la TSU), compromiso sospechoso o pérdida o fallo de la calibración, Sectigo no emitirá sellos de tiempo hasta que se tomen medidas para recuperarse del compromiso.

7.14. Planes de terminación y terminación de la TSA

En caso de terminación de las operaciones de la TSA por cualquier motivo, Sectigo proporcionará un aviso oportuno y la transferencia de responsabilidades a las entidades sucesoras, el mantenimiento de registros y las reparaciones. Sectigo tomará los siguientes pasos, cuando sea posible:

- Notificación al organismo supervisor antes de la rescisión
- Proporcionar a los Suscriptores, terceras partes de confianza y otras partes afectadas con noventa (90) días de anticipación de su intención de dejar de actuar como TSA.
- Revocación de todos los certificados de TSU.
- Hacer arreglos razonables para preservar sus registros de acuerdo con este TSPPS.
- Se reserva el derecho de proporcionar acuerdos de sucesión para la reemisión de sellos de tiempo a una TSA sucesora que tenga todos los permisos relevantes para hacerlo y cumpla con todas las reglas necesarias, mientras que su operación es al menos tan segura como la de Sectigo.
- La destrucción de las claves privadas de las TSU, incluidas las copias de seguridad.

Los requisitos de este artículo podrán ser modificados por contrato, en la medida en que tales modificaciones afecten únicamente a las partes contratantes.

Este plan se verifica, revisa y actualiza anualmente.

7.15. Cumplimiento

Las prácticas especificadas en este TSPPS han sido diseñadas para cumplir o exceder los requisitos de estándares de la industria generalmente aceptados y en desarrollo, incluidos ETSI EN 319401 y ETSI EN 319 421 y otros estándares de la industria relacionados con el funcionamiento de una TSA, como el IETF RFC 3161/5816.

Sectigo también cumple con la normativa eIDAS.

Un auditor externo independiente evalúa el cumplimiento de Sectigo con los estándares ETSI y la normativa eIDAS.

7.15.1. Frecuencia o circunstancias de la evaluación

La auditoría exige que el período se divida en una secuencia ininterrumpida de períodos de auditoría. Un período de auditoría no debe exceder los dos años de duración.

7.15.2. Identidad / calificaciones del auditor

Un CAB acreditado realiza la auditoría de Sectigo. Un CAB significa una persona física, entidad legal o grupo de personas físicas o entidades legales que colectivamente poseen las siguientes calificaciones y habilidades:

- Independencia del tema de la auditoría;
- La capacidad de realizar una auditoría que aborde los criterios especificados en un esquema de auditoría elegible;
- Emplea a personas que tienen competencia en el examen de tecnología de infraestructura de clave pública, herramientas y técnicas de seguridad de la información, tecnología de la información y auditoría de seguridad, y la función de certificación de terceros;
- Obligado por la ley, la regulación gubernamental o el código de ética profesional

7.15.3. Relación del evaluador con la entidad evaluada

El auditor o CAB es independiente de Sectigo y no tiene un interés financiero, una relación comercial o un curso de trato que pudiera crear un conflicto de intereses o crear un sesgo significativo (a favor o en contra) de Sectigo.

7.15.4. Temas cubiertos por la evaluación

El CAB evalúa el cumplimiento del componente auditado, en todo o en parte de la implementación de:

- la documentación (TSPPS, políticas, procedimientos, …);
- los componentes técnicos de la TSA

Antes de cada auditoría, el CAB sugiere una lista de componentes y procedimientos que desean verificar. Usan esto para desarrollar el plan de auditoría detallado.

7.15.5. Comunicación de resultados

Sectigo pondrá el informe de auditoría a disposición del Órgano de Control encargado de calificar y certificar el servicio. No se requiere que Sectigo ponga a disposición del público ningún hallazgo de auditoría general que no afecte la opinión general de auditoría.

8. Requisitos adicionales según el reglamento eIDAS

8.1. Certificado de clave pública TSU

Si se afirma que un sello de tiempo es un sello de tiempo electrónico cualificado según el Reglamento (UE) 910/2014, el certificado de clave (pública) de verificación de firma de TSU debe ser emitido por una autoridad de certificación que opere conforme a ETSI EN 319411-2.

Este es el identificador de objeto ASN.1 para afirmar que el token de sello de tiempo está cualificado

```
-- object identifiers
id-etsi-tsts OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4) etsi(0)
id-tst-profile(19422) 1 }
id-etsi-tsts-EuQCompliance OBJECT IDENTIFIER ::= { id-etsi-tsts 1 }
-- statements
esi4-qtstStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-tsts-EuQCompliance }
-- By inclusion of this statement the issuer claims that this
-- time-stamp token is issued as a qualified electronic time-stamp according to
-- the REGULATION (EU) No 910/2014.
```

8.2. TSA que emite sellos de tiempo electrónicos cualificados y no cualificados según el Reglamento (UE) 910/2014

Sectigo opera tres Autoridades de Sellado de Tiempo (TSA). Las TSA de Sectigo están diseñadas para proporcionar el tiempo exacto cuando se firma o sellan documentos o ficheros y para brindar la integridad necesaria a estos documentos o ficheros.

Las TSA no cualificadas que brindan servicios de sellado de tiempo se brindan desde diferentes URL y utilizan diferentes TSU identificadas por diferentes nombres de sujeto en su certificado de clave pública.

El servicio de sellado de tiempo Sectigo Authenticode está disponible en la URL:
http://timestamp.sectigo.com/authenticode

Sectigo también ofrece un TSA RFC3161, cuya URL es:

http://timestamp.sectigo.com/rfc3161

Si bien la TSA cualificada por Sectigo se proporciona desde:

http://timestamp.sectigo.com/qualified

Anexo A: Registro de cambios

Versión	Descripción	Fecha
1.0	Primer borrador de la versión	14 de Febrero de 2020
1.0.1	Dirección de oficina actualizada y persona de contacto	17 de Septiembre de 2020
1.0.2	Incluya el OID para las sellos de tiempo	14 de Octubre de 2020
1.0.3	Secciones actualizadas 4.3, 5.2, 7.6.2.2 y 8.2	20 de Octubre de 2020
1.0.4	Se actualizaron la sección 5.2 y el anexo B. Añadido un nuevo anexo C con la jerarquía de la TSA	22 de Octubre de 2020
1.0.5	Sección 5.2 actualizada sobre OID	23 de Octubre de 2020
1.0.6	Actualizaciones en los anexos B y C	23 de Octubre de 2020
1.0.7	Actualización sobre el TST, incluida la precisión y qcStatement y la adición de algunos laboratorios de estrato 1 UTC (k) en la sección 7.1.1	20 de Noviembre de 2020
1.0.8	Errores gramaticales menores corregidos. Clarificación en las secciones 6.6.2 y 7.7.1	15 de Marzo de 2022
1.0.9	Actualización de la sección 7.6.6 para incluir la renovación específica del certificado TSU y la clave privada Actualización de la sección 7.13 para no emitir tokens de marca de tiempo en caso de compromiso	13 de Enero de 2023
1.1.0	Referencias actualizadas Actualizaciones menores en las secciones 7.7.1 (nueva que reemplaza la genérica 7.7) y 7.8.2	27 de Octubre de 2023

Anexo B: Formato de solicitudes y respuestas

Formato de solicitud

El formato de envío de las solicitudes sigue el siguiente esquema:

Tipo de contenido: aplicación / consulta de sello de tiempo

Método: POST

Longitud del contenido: obligatorio

Contiene la solicitud de sello de tiempo en ASN.1, codificada en DER

Los campos opcionales de acuerdo con la especificación RFC3161 se tratan de la siguiente manera:

Campo	Tratamiento
Nonce	Optional. If present, the response contains the same value
reqPolicy	No use
certReq	No use
Extensions	No use

Formato de respuesta

Si la solicitud no se puede procesar, se devuelve una respuesta http que indica un código de error cuando no puede responder con un sello de tiempo. Los posibles errores son:

Razón	Error	Descripción
Missing content-length field	411	CONTENT_LENGHT REQUIRED
Content-length too large	413	REQUEST ENTITY TOO LARGE
Incorrect content-type	415	UNSUPPORTED MEDIA TYPE
Data are not a timestamp request	400	BAD REQUEST
Server not responding	500	SERVER INTERNAL ERROR

Las respuestas utilizan el siguiente esquema:

Tipo de contenido: aplicación / sello de tiempo-respuesta

Método: POST

Longitud del contenido: obligatorio

Contiene la respuesta del sello de tiempo en ASN.1, codificada en DER

Los campos opcionales de acuerdo con la especificación RFC3161 se tratan de la siguiente manera:

Campo	**Tratamiento**
Time-stamp policy	OID
Ordering	False
Nonce	If comes with the request, return the same value
Certificates	TSA certificate. subCA certificate
Accuracy	0x01 seconds, unspecified millis, unspecified micros
Tsa	No present
extensions	esi4-qtstStatement-1 QC-STATEMENT

Anexo C: jerarquía de la TSA

Certificado raíz

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 7b24e01933c796dfc404ce01161f5373
Algoritmo de firma:	sha384WithRSAEncryption	
Editor:	nombre común	Sectigo Qualified Time Stamping Root R45
	Nombre de la Organización	Sectigo (Europa) SL
	nombre del país	ES
Validez (25 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Miércoles, 4 de octubre de 2045
Sujeto:	nombre común	Sectigo Qualified Time Stamping Root R45
	Nombre de la Organización	Sectigo (Europa) SL
	nombre del país	ES
Thumbprint		RSA: cb73944c042e53bfc4579d2f712f3eea99fe4307

Sellado de tiempo cualificado de Sectigo CA R35

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 0cda8301d3f3280e71cdb028a352c65b
Algoritmo de firma:	sha384WithRSAEncryption	
Editor:	nombre común	Sectigo Qualified Time Stamping Root R45
	Nombre de la Organización	Sectigo (Europa) SL
	nombre del país	ES
Validez (15 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Jueves, 4 de octubre de 2035
Sujeto:	nombre común	Sellado de tiempo cualificado de Sectigo CA R35
	Nombre de la Organización	Sectigo (Europa) SL
	nombre del país	ES
Thumbprint		RSA: 1d6318b5b7d9ba360d757ac955881bf17c750766