Política de certificados eIDAS de Sectigo

Sectigo
Versión 1.0.5
Efectivo: 22 de octubre de 2020
Rambla Catalunya, 86 3 1,
08008 Barcelona, España
www.sectigo.com

Aviso de copyright

Copyright Sectigo 2020. Todos los derechos reservados.

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) S.L.
Rambla Catalunya, 86 3 1,
08008 Barcelona, España
www.sectigo.com

SECTIGO

Contenido

1. INTRODUCCIÓN 12
1.1. Visión general 12
1.2. Nombre e identificación del documento 12
1.3. Participantes de PKI 12
1.3.1. Autoridades de certificación 12
1.3.2. Autoridades de registro 13
1.3.3. Suscriptores 14
1.3.4. Terceras partes de confianza 14
1.3.5. Otros participantes 14
1.4. Uso del certificado 14
1.4.1. Usos apropiados de los certificados 14
1.4.2. Usos prohibidos de certificados 14
1.5. Administración de políticas 14
1.5.1. Organización que administra el documento 15
1.5.2. Persona de contacto 15
1.5.3. Persona que determina la idoneidad de CP para la póliza 15
1.5.4. Procedimientos de aprobación de CP 15
1.6. Definiciones y siglas 15
1.6.1. Definiciones 15
1.6.2. Siglas 21
2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPOSITARIO 22
2.1. Repositorios 23
2.2. Publicación de información de certificación 23
2.3. Hora o frecuencia de publicación 23
2.4. Controles de acceso en repositorios 23
2.5. Exactitud de la información 23
3. IDENTIFICACIÓN Y AUTENTICACIÓN 24
3.1. Nombres 24
3.1.1. Tipos de nombres 24

3.1.2. Necesidad de que los nombres sean significativos 24
3.1.3. Anonimato o seudonimato de los suscriptores. 24
3.1.4. Reglas para interpretar varias formas de nombres 24
3.1.5. Unicidad de nombres 24
3.1.6. Reconocimiento, autenticación y función de las marcas comerciales 24
3.2. Validación de identidad inicial 25
3.2.1. Autenticación de la identidad de una persona física 25
3.2.2. Autenticación de la identidad de una persona jurídica 25
3.2.3. QWAC 25
3.2.4. PSD2 25
3.2.5. Método para demostrar la posesión de la clave privada 25
3.2.6. Validación de autoridad 26
3.2.7. Criterios de interoperación 26
3.2.8. Validación de la aplicación 26
3.3. Identificación y autenticación para solicitudes de renovación de claves 26
3.3.1. Identificación y autenticación para el cambio de clave de rutina 26
3.3.2. Identificación y autenticación para re-clave después de la revocación 26
3.4. Identificación y autenticación para solicitud de revocación 26
4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO 27
4.1. Solicitud de certificado 27
4.1.1. ¿Quién puede enviar una solicitud de certificado? 28
4.1.2. Proceso de inscripción y responsabilidades 28
4.2. Procesamiento de solicitud del certificado 28
4.2.1. Realización de funciones de identificación y autenticación 29
4.2.2. Aprobación o rechazo de solicitudes de certificados 29
4.2.3. Procesar las solicitudes de certificados 29
4.2.4. Autorización de la autoridad de certificación 29
4.3. Emisión de certificados 30
4.3.1. Acciones de la CA durante la emisión del certificado 30
4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado 31
4.3.3. Negarse a emitir un certificado 31
4.4. Aceptación del certificado 31

4.4.1. Conducta que constituye la aceptación del certificado ... 31
4.4.2. Publicación del certificado por la CA ... 31
4.4.3. Notificación de la emisión del certificado por parte de la CA a otras entidades ... 31
4.5. Par de claves y uso de certificados ... 32
4.5.1. Uso de certificado y clave privada del suscriptor ... 32
4.5.2. Uso de certificado y clave pública del tercero de confianza ... 32
4.6. Renovación del certificado ... 32
4.6.1. Circunstancia para la renovación del certificado ... 32
4.6.2. Quién puede solicitar la renovación ... 32
4.6.3. Procesamiento de solicitudes de renovación de certificados ... 32
4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor ... 32
4.6.5. Conducta que constituye la aceptación de un certificado de renovación ... 32
4.6.6. Publicación del certificado de renovación por parte de la CA ... 33
4.6.7. Notificación de la emisión del certificado por parte de la CA a otras entidades ... 33
4.7. Cambio de clave del certificado ... 33
4.7.1. Circunstancia para el cambio de clave del certificado ... 33
4.7.2. Quién puede solicitar la certificación de una nueva clave pública ... 33
4.7.3. Procesamiento de solicitudes de cambio de claves de certificados ... 33
4.7.4. Notificación de la emisión de un nuevo certificado al suscriptor ... 33
4.7.5. Conducta que constituye la aceptación de un certificado con clave nueva ... 33
4.7.6. Publicación del certificado con nueva clave por parte de la CA ... 34
4.7.7. Notificación de la emisión del certificado por parte de la CA a otras entidades ... 34
4.8. Modificación del certificado ... 34
4.9. Revocación y suspensión de certificados ... 34
4.9.1. Circunstancias para la revocación ... 34
4.9.2. Quién puede solicitar la revocación ... 36
4.9.3. Procedimiento de solicitud de revocación ... 37
4.9.4. Tiempo dentro del cual la CA debe procesar la solicitud de revocación ... 37
4.9.5. Requisito de verificación de revocación para los terceros de confianza ... 37
4.9.6. Frecuencia de emisión de CRL (si corresponde) ... 37
4.9.7. Latencia máxima para las CRL (si corresponde) ... 38
4.9.8. Disponibilidad de verificación del estado / revocación en línea ... 38

4.9.9. Requisitos de verificación de revocación en línea ... 38
4.10. Servicios del estado de los certificados ... 38
4.10.1. Características operativas ... 38
4.10.2. Servicio disponible ... 39
4.11. Fin de suscripción ... 39
5. CONTROLES OPERATIVOS, DE GESTIÓN Y DE INSTALACIONES ... 39
5.1. Controles físicos ... 39
5.1.1. Ubicación y construcción del sitio o CPD ... 39
5.1.2. Acceso físico ... 40
5.1.3. Energía y aire acondicionado ... 40
5.1.4. Exposiciones al agua ... 41
5.1.5. Prevención y protección contra incendios ... 41
5.1.6. Almacén de datos ... 41
5.1.7. Deposito de basura ... 41
5.1.8. Copia de seguridad fuera del sitio ... 41
5.2. Controles de procedimiento ... 42
5.2.1. Roles confiables ... 42
5.2.2. Número de personas necesarias por tarea ... 43
5.2.3. Identificación y autenticación para cada rol ... 43
5.3. Controles de personal ... 44
5.3.1. Requisitos de calificaciones, experiencia y autorización ... 44
5.3.2. Procedimientos de verificación de antecedentes ... 44
5.3.3. Requisitos de formación ... 45
5.3.4. Frecuencia de formación ... 45
5.3.5. Sanciones por acciones no autorizadas ... 45
5.3.6. Requisitos del contratista independiente ... 46
5.3.7. Documentación suministrada al personal ... 46
5.4. Procedimientos de registro de auditoría ... 46
5.4.1. Tipos de eventos registrados ... 46
5.4.2. Registro de frecuencia de procesamiento ... 47
5.4.3. Período de retención del registro de auditoría ... 47
5.4.4. Protección del registro de auditoría ... 47

5.4.5. Procedimientos de copia de seguridad del registro de auditoría 47
5.4.6. Sistema de realización de auditorías (interno vs. externo) 48
5.4.7. Evaluaciones de vulnerabilidad 48
5.5. Archivo de registros 48
5.5.1. Tipos de registros archivados 48
5.5.2. Periodo de conservación del archivo 48
5.5.3. Protección del archivo 49
5.5.4. Procedimientos de respaldo de archivos 49
5.5.5. Requisitos para el sellado de tiempo de los registros 49
5.5.6. Sistema de recolección de archivos (interno o externo) 50
5.5.7. Procedimientos para obtener y verificar información de archivo 50
5.6. Cambio de clave 50
5.7. Compromiso y recuperación ante desastres 50
5.7.1. Procedimientos de manejo de incidentes y compromisos 50
5.7.2. Los recursos informáticos, el software y / o los datos están dañados 51
5.7.3. Procedimientos de compromiso de clave privada de la CA 51
5.7.4. Procedimientos de compromiso de algoritmos 51
5.7.5. Capacidades de continuidad empresarial después de un desastre 51
5.8. Terminación del TSP 52
6. CONTROLES DE SEGURIDAD TÉCNICA 52
6.1. Generación e instalación de pares de claves 52
6.1.1. Generación de pares de claves 52
6.1.2. Entrega de clave privada al suscriptor 53
6.1.3. Entrega de clave pública al emisor del certificado 54
6.1.4. Entrega de clave pública de la CA a los terceros de confianza 54
6.1.5. Tamaños de clave 54
6.1.6. Generación de parámetros de clave pública y control de calidad 55
6.1.7. Propósitos de uso clave 55
6.2. Protección de clave privada y controles del módulo criptográfico 56
6.2.1. Estándares y controles de módulos criptográficos 56
6.2.2. Transferencia de clave privada hacia o desde un módulo criptográfico 56
6.2.3. Almacenamiento de clave privada en módulo criptográfico 56

6.2.4. Método de activación de la clave privada ... 56
6.2.5. Método para desactivar la clave privada ... 57
6.2.6. Método de destrucción de la clave privada ... 58
6.2.7. Clasificación del módulo criptográfico ... 58
6.3. Otros aspectos de la gestión de los pares de claves ... 58
6.3.1. Archivo de clave pública ... 58
6.3.2. Períodos operativos del certificado y períodos de uso de pares de claves ... 58
6.4. Datos de activación ... 58
6.4.1. Generación e instalación de datos de activación ... 59
6.4.2. Protección de datos de activación ... 59
6.5. Controles de seguridad informática ... 59
6.5.1. Requisitos técnicos específicos de seguridad informática ... 59
6.6. Controles técnicos del ciclo de vida ... 59
6.6.1. Controles de desarrollo del sistema ... 59
6.6.2. Controles de gestión de seguridad ... 60
6.7. Controles de seguridad de la red ... 60
6.8. Sellado de tiempo ... 61
7. PERFILES DE CERTIFICADOS, CRL Y OCSP ... 61
7.1. Perfil de certificado ... 61
7.1.1. Número (s) de versión ... 62
7.1.2. Extensiones de certificado ... 62
7.1.3. Identificadores de objetos de algoritmo ... 62
7.1.4. Formas de nombres ... 62
7.1.5. Identificador de objeto de política de certificado ... 62
7.1.6. Sintaxis y semántica de los policy qualifiers ... 62
7.2. Perfil de CRL ... 62
7.2.1. Número (s) de versión ... 63
7.2.2. Extensiones de entrada de CRL y CRL ... 63
7.3. Perfil OCSP ... 63
7.3.1. Número (s) de versión ... 64
8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES ... 64
8.1. Frecuencia o circunstancias de la evaluación ... 64

8.2. Identidad / calificaciones del auditor ... 64
8.3. Relación del auditor con la entidad evaluada ... 64
8.4. Temas cubiertos por la auditoria ... 64
8.5. Acciones tomadas como resultado de una deficiencia ... 65
8.6. Comunicación de resultados ... 65
8.7. Auto auditorías ... 65
9. OTROS ASUNTOS LEGALES Y COMERCIALES ... 66
9.1. Tarifa ... 66
9.1.1. Tarifas de emisión o renovación de certificados ... 66
9.1.2. Tarifas de acceso al certificado ... 66
9.1.3. Tarifas de acceso a la información de estado o revocación ... 66
9.2. Responsabilidad financiera ... 66
9.2.1. Cobertura del seguro ... 66
9.3. Confidencialidad de la información comercial ... 66
9.3.1. Alcance de la información confidencial ... 66
9.3.2. Información que no está dentro del alcance de la información confidencial ... 67
9.3.3. Responsabilidad de proteger la información confidencial ... 67
9.4. Privacidad de la información personal ... 67
9.4.1. Plan de privacidad ... 67
9.4.2. Información tratada como confidencial ... 67
9.4.3. Información no considerada confidencial ... 67
9.4.4. Responsabilidad de proteger la información confidencial ... 67
9.4.5. Aviso y consentimiento para usar información confidencial ... 67
9.4.6. Divulgación de conformidad con un proceso judicial o administrativo ... 68
9.5. Derechos de propiedad intelectual ... 68
9.6. Representaciones y garantías ... 68
9.6.1. Representaciones y garantías de la CA ... 68
9.6.2. Representaciones y garantías de la RA ... 69
9.6.3. Declaraciones y garantías de los suscriptores ... 69
9.6.4. Declaraciones y garantías de las partes confiables ... 70
9.7. Renuncias de garantías ... 71
9.7.1. Aptitud para un propósito particular ... 71

9.7.2. Otras garantías ... 71
9.8. Limitaciones de responsabilidad ... 72
9.8.1. Limitaciones de daños y pérdidas ... 72
9.8.2. Exclusión de ciertos elementos de daños. ... 72
9.9. Indemnizaciones ... 73
9.9.1. Indemnización por suscriptor ... 73
9.10. Duración y Terminación ... 73
9.10.1. Término ... 73
9.10.2. Terminación ... 73
9.10.3. Efecto de terminación y supervivencia ... 74
9.11. Avisos individuales y comunicaciones con los participantes ... 74
9.12. Enmiendas ... 74
9.12.1. Procedimiento de modificación ... 75
9.12.2. Mecanismo y período de notificación ... 75
9.12.3. Circunstancias bajo las cuales se debe cambiar el OID ... 75
9.13. Disposiciones de resolución de disputas ... 75
9.14. Ley aplicable, interpretación y jurisdicción ... 75
9.14.1. Ley que rige ... 75
9.14.2. Interpretación ... 76
9.14.3. Jurisdicción ... 76
9.15. Cumplimiento de la ley aplicable ... 76
9.16. Otras disposiciones ... 76
9.16.1. Acuerdo completo ... 76
9.16.2. Asignación ... 76
9.16.3. Divisibilidad ... 77
9.16.4. Ejecución (honorarios de abogados y renuncia de derechos) ... 77
9.16.5. Fuerza mayor ... 77
9.16.6. Conflicto de reglas ... 77
9.17. Otras provisiones ... 78
9.17.1. Responsabilidad del suscriptor con los terceros de confianza ... 78
9.17.2. Deber de supervisar a los agentes ... 78
9.17.3. Propiedad ... 78

9.17.4. Interferencia con la implementación de Sectigo 78
9.17.5. Elección del método criptográfico 78
9.17.6. Limitaciones de las asociaciones de Sectigo 78
9.17.7. Obligaciones del suscriptor 79
Apéndice A: ChangeLog 80

1. INTRODUCCIÓN

1.1. Visión general

Este documento define la Política de certificados para Sectigo eIDAS PKI que rige la emisión de certificados cualificados.

Sectigo cumple con el reglamento de la UE 910/2014 (también conocido como eIDAS), con los estándares ETSI y con la versión actual de los requisitos básicos (BR) y las directrices EV (EVG) del CAB Forum. En el caso de cualquier inconsistencia entre este CP y el BR o EVG, el BR o EVG tienen prioridad sobre este documento cuando los certificados cualificados emitidos están destinados a autenticar sitios web sobre el protocolo SSL / TLS.

Sectigo extiende, bajo acuerdo, la membresía de su PKI a terceros aprobados conocidos como Autoridades de Registro (RA). La red internacional de RA de Sectigo comparte las políticas, las prácticas y la infraestructura de CA de Sectigo para emitir certificados cualificados de Sectigo.

1.2. Nombre e identificación del documento

Este documento es la Política de certificados (CP) eIDAS de Sectigo. Describe los principios y prácticas legales, comerciales y técnicos que Sectigo emplea para proporcionar servicios de certificación cualificados para aplicaciones PKI que incluyen, entre otros, la aprobación, emisión, uso y gestión de certificados digitales y el mantenimiento de un certificado X.509 basado en Infraestructura de clave pública (PKI) de acuerdo con las políticas de certificados determinadas por Sectigo. También define los procesos de certificación subyacentes para los suscriptores y describe las operaciones del repositorio de Sectigo. El documento CP también es un medio de notificación de roles y responsabilidades para las partes involucradas en prácticas basadas en certificados dentro de Sectigo eIDAS PKI.

El document Sectigo eIDAS CP es una declaración pública de las prácticas de Sectigo y las condiciones de emisión, revocación y renovación de un certificado cualificado emitido bajo la propia jerarquía de Sectigo.

1.3. Participantes de PKI

Esta sección identifica y describe algunas de las entidades que participan dentro de Sectigo eIDAS PKI. Sectigo cumple con este CP y otras obligaciones que asume a través de contratos adyacentes cuando presta sus servicios.

1.3.1. Autoridades de certificación

Sectigo proporciona servicios de certificados dentro de Sectigo eIDAS PKI. Sectigo hará:

- Cumplir sus operaciones con el CP (u otra divulgación de prácticas comerciales de CA), ya que las mismas pueden ser modificadas de vez en cuando por enmiendas publicadas en el repositorio,
- Emitir y publicar certificados de manera oportuna de acuerdo con los tiempos de emisión establecidos en esta CP,

- Al recibir una solicitud válida para revocar el certificado de una persona autorizada para solicitar la revocación utilizando los métodos de revocación detallados en este CP,
- Publicar las CRL de forma regular, de acuerdo con la Política de Certificados aplicable y con las disposiciones descritas en este CP,
- Distribuir los certificados emitidos de acuerdo con los métodos detallados en este CP,
- Actualizar las CRL de manera oportuna como se detalla en este CP,

1.3.1.1. Autoridad de políticas

Esta entidad decide que un conjunto de requisitos para la emisión y el uso de certificados son suficientes para una aplicación determinada. La Autoridad de Políticas (PA):

- Establece y mantiene este documento CP.
- Aprueba el establecimiento de relaciones de confianza con PKI externas que ofrecen una garantía adecuadamente comparable.
- Asegura que todos los aspectos de los servicios, operaciones e infraestructura de CA como se describen en la CPS se realicen de acuerdo con los requisitos, representaciones y garantías de la CP.

1.3.2. Autoridades de registro

Las autoridades de registro (RA) recopilan y verifican la identidad y la información de cada suscriptor que se ingresará en el certificado de clave pública del suscriptor. La RA realiza su función de acuerdo con una CPS aprobada por la Autoridad de Políticas. La RA es responsable de:

- El proceso de registro
- El proceso de identificación y autenticación.

Las RA actúan localmente dentro de su propio contexto de asociaciones geográficas o comerciales con la aprobación y autorización de Sectigo de acuerdo con las prácticas y procedimientos de Sectigo.

Las RA pueden estar habilitados para realizar la validación de parte o toda la información de identidad del sujeto, pero no pueden realizar la validación del control de dominio en el caso de los certificados SSL.

Las RA solo pueden realizar sus tareas de validación a partir de sistemas pre aprobados que se identifican a la CA por diversos medios que siempre incluyen, entre otros, la lista blanca de la dirección IP desde la que opera la RA.

Sectigo opera una serie de CA intermedias desde las cuales emite certificados cualificados para los cuales una parte de la validación ha sido realizada por una autoridad de registro. Algunas de las CA intermedias se dedican al trabajo de una única RA, mientras que otras se dedican al trabajo de múltiples RA relacionadas.

Personal de la autoridad de registro: El personal de RA son las personas que desempeñan funciones de confianza que operan y gestionan los componentes de RA.

1.3.3. Suscriptores

Los suscriptores de los servicios de Sectigo son personas o empresas que utilizan la PKI en relación con las transacciones y comunicaciones compatibles con Sectigo. Los suscriptores son partes que se identifican en un certificado y poseen la clave privada correspondiente a la clave pública que figura en el certificado. Antes de la verificación de la identidad y la emisión de un certificado, un suscriptor es un solicitante de los servicios de Sectigo.

1.3.4. Terceras partes de confianza

Una tercera parte que confía es una entidad que se basa en la validez de la vinculación del nombre del suscriptor a una clave pública. La tercera parte que confía utiliza un certificado de suscriptor para verificar o establecer la identidad y el estado del suscriptor. Una tercera parte que confía es responsable de decidir si verificar la validez del certificado, o cómo, mediante la verificación de la información apropiada sobre el estado del certificado. Una tercera parte que confía puede utilizar la información del certificado para determinar la idoneidad del certificado para un uso particular.

1.3.5. Otros participantes

Las CA y RA que operan bajo el CP pueden requerir los servicios de otras autoridades de seguridad, comunidad y aplicación. La CPS identificará a las partes responsables de proporcionar dichos servicios y los mecanismos utilizados para respaldar estos servicios.

1.4. Uso del certificado

1.4.1. Usos apropiados de los certificados

Sectigo ofrece una gama de distintos tipos de certificados cualificados. Los diferentes tipos tienen diferentes usos previstos y diferentes políticas.

El uso específico del certificado se definirá en la CPS.

1.4.2. Usos prohibidos de certificados

Se prohíbe el uso de certificados en la medida en que el uso sea incompatible con la ley aplicable. Se prohíbe el uso de certificados como equipo de control en circunstancias peligrosas o para usos que requieran un desempeño a prueba de fallos, como la operación de instalaciones nucleares, sistemas de comunicación o navegación de aeronaves, sistemas de control de tráfico aéreo o sistemas de control de armas, donde la falla podría conducir directamente a muerte, lesiones personales o daños graves a personas o propiedad.

1.5. Administración de políticas

La información que se encuentra en esta sección incluye la información de contacto de la organización responsable de la redacción, registro, mantenimiento, actualización y aprobación del Sectigo eIDAS CP.

1.5.1. Organización que administra el documento

La autoridad de políticas de Sectigo mantiene este CP, los acuerdos relacionados y las políticas de certificación a las que se hace referencia en este documento.

1.5.2. Persona de contacto

Se puede contactar con la autoridad de política de Sectigo en la siguiente dirección:

Autoridad de políticas de Sectigo
3.er piso, 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, Reino Unido
Tel: +44 (0) 161 874 7070
Fax: +44 (0) 161877 1767
URL: https://sectigo.com/
Correo electrónico: legalnotices@sectigo.com

1.5.3. Persona que determina la idoneidad de CP para la póliza

La Autoridad de Políticas de Sectigo es responsable de determinar la idoneidad de las políticas de certificados ilustradas en este CP. La Autoridad de Políticas de Sectigo también es responsable de determinar la idoneidad de los cambios propuestos al CP antes de la publicación de una edición enmendada.

1.5.4. Procedimientos de aprobación de CP

La Autoridad de Políticas de Sectigo aprueba este CP y cualquier cambio, enmienda o adición posterior.

1.6. Definiciones y siglas

1.6.1. Definiciones

Solicitante: Significa la persona física o jurídica que solicita (o busca la renovación) de un certificado. Una vez que se emite el certificado, se hace referencia al solicitante como suscriptor. Para los certificados emitidos a dispositivos, el solicitante es la entidad que controla u opera el dispositivo mencionado en el certificado, incluso si el dispositivo envía la solicitud de certificado real.

Representante del solicitante: Significa una persona física o patrocinador que es el solicitante, empleado por el solicitante o un agente autorizado que tiene autoridad expresa para representar al solicitante: (i) que firma y presenta o aprueba una solicitud de certificado en nombre del solicitante, y / o (ii) quien firma y envía un Acuerdo de Suscriptor en nombre del solicitante, y / o (iii) quien reconoce y acepta los Términos de Uso del certificado en nombre del solicitante cuando el solicitante es un Afiliado de la CA.

Proveedor de software de aplicación: Un proveedor de software de navegador de Internet u otro software de aplicación de parte de confianza que muestra o utiliza certificados e incorpora certificados raíz.

Informe de auditoría: Significa un informe de un auditor cualificado que expresa la opinión del auditor cualificado sobre si los procesos y controles de una entidad cumplen con la regulación eIDAS y los requisitos de las normas ETSI.

Representante organizativo autorizado: Una persona (potencialmente entre varias) dentro de una organización que está autorizada a dar fe de identidades personales y no personales. Cualquier AOR en particular no está vinculado permanentemente a ninguna identidad particular que no sea de persona; la CA solo debe asegurarse de que el AOR esté legítimamente asociado con la organización, y que el AOR esté identificado con autoridad para solicitar certificados para la organización.

Nombre de dominio de autorización: Significa el nombre de dominio utilizado para obtener la autorización para la emisión de certificados para un FQDN determinado.

Requisitos básicos (BR): Requisitos básicos de CA / Browser Forum para la emisión y gestión de certificados de confianza pública, publicados en https://cabforum.org/

Restricciones básicas: Significa una extensión que especifica si el sujeto del certificado puede actuar como una CA o solo como una entidad final.

Certificado: Significa un documento electrónico que utiliza una firma digital para vincular una clave pública y una entidad.

Sistema de gestión de certificados: Hace referencia a un sistema utilizado por Sectigo para procesar, aprobar la emisión o almacenar certificados o información sobre el estado de los certificados, incluida la base de datos, el servidor de la base de datos y el almacenamiento.

Gestión de certificados: Significa las funciones que incluyen, entre otras, las siguientes: verificación de la identidad de un solicitante de un certificado; autorizar la emisión de certificados; emisión de certificados; revocación de certificados; listado de certificados; distribuir certificados; publicación de certificados; almacenar certificados; almacenar claves privadas; custodia de claves privadas; generación, emisión, desmantelamiento y destrucción de pares de claves; recuperar certificados de acuerdo con su uso particular previsto; y verificación del dominio de un solicitante de certificado.

Administrador de certificados: Significa el software emitido por Sectigo y utilizado por los suscriptores para descargar certificados.

Declaración de prácticas de certificación: Uno de los varios documentos que forman el marco de gobierno en el que se crean, emiten, gestionan y utilizan los certificados.

Política de certificado: Significa una declaración del emisor que corresponde al uso prescrito de un certificado digital dentro de un contexto de emisión.

Servidor de estado del certificado: Una entidad de confianza que proporciona verificación en línea a una parte que confía del estado de revocación de un certificado sujeto y también puede proporcionar información de atributos adicionales para el certificado sujeto.

Sistemas de certificados: Hace referencia al sistema utilizado por Sectigo o un tercero delegado para proporcionar verificación de identidad, registro e inscripción, aprobación de certificado, emisión, estado de validez, soporte y otros servicios relacionados con la PKI.

Organismo de evaluación de la conformidad: organismo que realiza servicios de evaluación de la conformidad que está acreditado como competente para llevar a cabo la evaluación de la conformidad de un proveedor de servicios de confianza cualificado y los servicios de confianza cualificados que presta.

Contacto de dominio: Significa el Registrante del Nombre de Dominio, el contacto técnico o el contrato administrativo (o el equivalente bajo un ccTLD) como se indica en el registro de WHOIS del Nombre de Dominio Base o en un registro SOA del Sistema de Nombres de Dominio (DNS).

Nombre de dominio: Significa la etiqueta asignada a un nodo en el Sistema de nombres de dominio.

Registrante del nombre de dominio: Hace referencia a la (s) persona (s) o entidad (es) registradas con un Registrador de nombres de dominio que tienen derecho a controlar cómo se usa un Nombre de dominio, como la persona física o Entidad legal que aparece como el "Registrante" por WHOIS o el Registrador de nombres de dominio y, a veces, denominado "propietario" de un nombre de dominio.

Registrador de nombres de dominio: Significa una persona o entidad que registra Nombres de Dominio bajo los auspicios de o por acuerdo con: (i) la Corporación de Internet para la Asignación de Nombres y Números (ICANN), (ii) una autoridad / registro nacional de Nombres de Dominio, o (iii) un Centro de información de la red (incluidos sus afiliados, contratistas, delegados, sucesores o cesionarios).

Firma electrónica: significa datos en formato electrónico que se adjuntan o se asocian lógicamente con otros datos en formato electrónico y que el firmante utiliza para firmar;

Sello electrónico: significa datos en formato electrónico, que se adjuntan o se asocian lógicamente con otros datos en formato electrónico para garantizar el origen y la integridad de estos últimos;

Directiva de servicios de pago de la UE 2015/2366: Esta directiva proporciona la base jurídica para un mayor desarrollo de un mercado interior mejor integrado para los pagos electrónicos dentro de la UE. También proporciona la plataforma legal necesaria para la zona única de pagos europea (SEPA). Deroga la directiva 2007/64 / CE.

Reglamento UE 910/2014: Este Reglamento sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el mercado interior (Reglamento eIDAS) adoptado el 23 de julio de 2014 proporciona un entorno regulatorio predecible para permitir interacciones electrónicas seguras y fluidas entre empresas, ciudadanos y autoridades públicas. Este reglamento simplifica y estandariza los sistemas de interacciones electrónicas en toda Europa para ayudar a crear un "mercado digital único".

Reglamento de la UE 2016/679: Este reglamento sobre la protección de las personas físicas con respecto al procesamiento de datos personales y de la libre circulación de dichos datos (GDPR) proporciona un entorno normativo para proteger los derechos y libertades fundamentales de las personas físicas para la protección de sus datos personales.

Directrices EV (EVG): Las Directrices de CA / Browser Forum para la emisión y gestión de certificados de validación extendida, publicadas en https://cabforum.org/

Sistema de soporte interno / frontal: Hace referencia a un sistema con una dirección IP pública, que incluye un servidor web, un servidor de correo, un servidor DNS, un servidor de salto o un servidor de autenticación.

Periodo de gracia: Significa el período durante el cual el suscriptor debe realizar una solicitud de revocación.

Sistema emisor: Significa un sistema utilizado para firmar certificados o información sobre el estado de validez.

Persona o entidad jurídica: Significa una asociación, corporación, sociedad, propiedad, fideicomiso, entidad gubernamental u otra entidad con personalidad jurídica en el sistema legal de un país.

Autoridad política: Significa la entidad encargada del mantenimiento y publicación de este CP.

Política de privacidad: Hace referencia a la última versión del documento publicado de Sectigo titulado como tal, que describe las políticas y prácticas de Sectigo en la recopilación, el uso y la protección de la información personal, y al que se puede acceder en el siguiente sitio web: https://www.sectigo.com/privacy-policy/.

Clave privada: Significa la clave, de un par de claves, que es mantenida en secreto por el titular del par de claves, y que se utiliza para crear firmas digitales y / o para desencriptar registros electrónicos o archivos que fueron encriptados con la correspondiente Clave Pública.

Clave pública: Significa la clave, de un par de claves, que puede ser divulgada públicamente por el titular de la correspondiente Clave Privada y que es utilizada por una Parte de Confianza para verificar firmas digitales creadas con la correspondiente Clave Privada del titular y / o para encriptar mensajes para que puedan ser descifrado sólo con la clave privada correspondiente del titular.

Certificado cualificado: En el contexto del Reglamento (UE) No 910/2014 (eIDAS), significa un certificado que cumple con los requisitos establecidos en este reglamento.

Certificado cualificado para firma electrónica: En el contexto del Reglamento (UE) n.o 910/2014 (eIDAS), se entiende un certificado de firma electrónica emitido por un proveedor de servicios de confianza cualificado.

Certificado cualificado para sello electrónico: En el contexto del Reglamento (UE) n.o 910/2014 (eIDAS), significa un certificado para un sello electrónico emitido por un proveedor de servicios de confianza cualificado.

Sello electrónico cualificado: significa un sello electrónico avanzado, que es creado por un dispositivo de creación de sello electrónico cualificado, y que se basa en un certificado cualificado para sello electrónico;

Firma electrónica cualificada: significa una firma electrónica avanzada que es creada por un dispositivo de creación de firma electrónica cualificado, y que se basa en un certificado cualificado para firmas electrónicas;

Dispositivo cualificado de creación de sello / firma electrónica: En el contexto del Reglamento (UE) n.o 910/2014 (eIDAS), se entiende un dispositivo de creación de sello o firma electrónica que cumple los requisitos estipulados en el Anexo II del Reglamento eIDAS.

Proveedor de servicios de confianza cualificado: Una persona física o jurídica que está reconocida por un organismo de supervisión nacional de un estado miembro de la Unión Europea para proporcionar (un subconjunto de) servicios de confianza cualificados según se define en el Reglamento eIDAS.

Certificado de autenticación de sitio web cualificado: En el contexto del Reglamento (UE) n.o 910/2014 (eIDAS), se entiende un certificado para identificar un sitio web emitido por un proveedor de servicios de confianza cualificado. Este certificado crea un vínculo seguro entre un sitio web y un navegador. Asegurándose de que todos los datos pasados entre los dos permanezcan privados y seguros

Valor aleatorio: Significa un valor especificado por Sectigo para el solicitante que exhibe al menos 112 bits de entropía.

Método de comunicación confiable: Hace referencia a un método de comunicación, como una dirección de entrega postal / de mensajería, un número de teléfono o una dirección de correo electrónico, que se verificó utilizando una fuente distinta al representante del solicitante.

Tercera parte de confianza: Significa una entidad que se basa en la información contenida en el certificado.

Acuerdo de los terceros de confianza: significa un acuerdo entre Sectigo y un tercero de confianza que debe ser leído y aceptado por ese tercero antes de validar, confiar o usar un certificado y está disponible para referencia en el repositorio.

Renovación: Realizar un nuevo pedido de un certificado que tenga la misma información de asunto para el que el suscriptor posea un certificado vigente y válido emitido por Sectigo. Por lo general, esto se hace <= 90 días antes de la expiración de los certificados actuales.

Reemplazo: Solicitar la emisión de un nuevo certificado para reemplazar un certificado válido vigente emitido por Sectigo sin realizar un nuevo pedido.

Repositorio: Significa el repositorio de Sectigo, disponible en https://www.sectigo.com/legal/

Solicitar token: Significa un valor derivado de un método especificado por Sectigo que vincula una demostración de control a la solicitud de certificado.

Sistema de CA raíz: Significa un sistema utilizado para crear un certificado raíz o para generar, almacenar o firmar con la clave privada asociada con un certificado raíz.

Sistema de soporte de seguridad: Hace referencia a un sistema que se utiliza para proporcionar funciones de soporte de seguridad, como autenticación, control de límites de red, registro de auditoría, reducción y análisis de registros de auditoría, escaneo de vulnerabilidades y antivirus.

Abonado: Significa una entidad a la que se le ha emitido un certificado.

Acuerdo de suscriptor: Significa un acuerdo que debe ser leído y aceptado por un solicitante antes de solicitar un certificado. El Acuerdo de suscripción es específico para el tipo de producto de certificado digital que se presenta durante el proceso de pedido en línea del producto y está disponible para referencia en el repositorio.

Servicio de confianza: servicio electrónico para:

- creación, verificación y validación de firmas digitales y certificados relacionados;
- creación, verificación y validación de sellos de tiempo y certificados relacionados;
- entrega certificada y certificados relacionados;
- creación, verificación y validación de certificados para la autenticación de sitios web; o
- conservación de firmas digitales o certificados relacionados con dichos servicios.

Proveedor de servicios de confianza: entidad que proporciona uno o más servicios de confianza

Proveedor de certificados raíz de confianza: Un proveedor de software de aplicación que mantiene una base de datos de certificados raíz de confianza y los requisitos de CA para ser incluido en ella, que normalmente se distribuye como parte de un navegador web o sistema operativo.

X.509: Significa el estándar ITU-T para certificados y su marco de autenticación correspondiente.

1.6.2. Siglas

AOR: Representante autorizado de la organización

BR: Requisitos básicos

CA: Autoridad de certificación

CAB: Organismo de evaluación de la conformidad

CPS: Declaración de prácticas de certificación

CRL (s): Lista (s) de revocación de certificados

CSR: Solicitud de firma de certificado

CSS: Servidor de estado de certificado

DN: Nombre distinguido

DSA: Algoritmo de firma digital

ECDSA: Algoritmo de firma digital de curva elíptica

eIDAS: Servicios electrónicos de identificación, autenticación y confianza

ETSI: Instituto Europeo de Normas y Telecomunicaciones

EPKI: Gerente de infraestructura de clave pública empresarial

EVG: Directrices EV

FIPS PUB: Publicación de estándares federales de procesamiento de información

FQDN: Nombre de dominio completo

FTP: Protocolo de transferencia de archivos

HSM: Módulo de seguridad de hardware

HTTP: Protocolo de Transferencia de Hipertexto

ICANN: Corporación de Internet para la Asignación de Nombres y Números

ITU: Unión Internacional de Telecomunicaciones

ITU-T: Sector de Normalización de las Telecomunicaciones de la UIT

MDC: Certificado de dominio múltiple

NIST: Instituto Nacional de Estándares y Tecnología

OCSP: Protocolo de estado de certificado en línea

PAC: Certificado de autenticación personal

PIN: Número de identificación personal

PKI: Infraestructura de Clave Pública

PKIX: Infraestructura de clave pública (basada en certificados digitales X.509)

PKCS: Estándar de criptografía de clave pública

PSD2: Directiva de servicios de pago 2

QSCD: Dispositivo de creación de sello / firma cualificado

QTSP: Proveedor de servicios de confianza cualificado

QWAC: Certificado de autenticación de sitio web cualificado

RA (s): Autoridad (es) de registro

RFC: Solicitud de comentarios

RSA: Rivest Shamir Adleman

SAN: Nombre alternativo del sujeto

SHA: Algoritmo hash seguro

SGC: Criptografía cerrada por servidor

S / MIME: Extensión (es) de correo de Internet seguro / multipropósito

SSL: Capa de sockets seguros

TLS: Transport Layer Security

TSA: Autoridad de Sellado de Tiempo

TSP: Proveedor de servicios de confianza

UTC: Hora universal coordinada

URL: Localizador Uniforme de Recursos

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPOSITARIO

Sectigo publica este CP y los documentos asociados en el Repositorio. La Autoridad de Políticas de Sectigo mantiene el Repositorio de Sectigo. Todas las actualizaciones, modificaciones y

promociones legales se registran de acuerdo con los procedimientos de registro a los que se hace referencia en la sección 5.4 de este CP.

La información crítica publicada puede actualizarse de vez en cuando según lo prescrito en este CP. Dichas actualizaciones se indican mediante la numeración de versión adecuada y la fecha de publicación en cualquier versión actualizada.

2.1. Repositorios

Sectigo publica un repositorio de avisos legales sobre sus servicios de PKI, incluyendo este CP, acuerdos y avisos, referencias dentro de este CP, así como cualquier otra información que considere esencial para sus servicios. Se puede acceder al repositorio en https://www.sectigo.com/legal/.

2.2. Publicación de información de certificación

Los servicios de certificados de Sectigo y el Repositorio son accesibles a través de varios medios de comunicación:

- En la red: www.sectigo.com
- Por correo electrónico: legalnotices@sectigo.com
- Por correo:

  Sectigo
  3.er piso, edificio 26 Exchange Quay, Trafford Road
  Salford, Greater Manchester, M5 3EQ, Reino Unido
  www.sectigo.com

2.3. Hora o frecuencia de publicación

La información de emisión y revocación de los certificados se publicará lo antes posible. Las versiones actualizadas o modificadas de los Acuerdos de suscriptor y los Acuerdos de los terceros de confianza generalmente se publican dentro de los siete días posteriores a la aprobación. Las versiones actualizadas o modificadas de Sectigo eIDAS CP se publican al menos una vez al año y de acuerdo con la sección 9.12 de este CP. Para conocer la frecuencia de emisión de CRL, consulte la sección 4.9.7 de este CP.

2.4. Controles de acceso en repositorios

Los documentos publicados en el Repositorio son de información pública y el acceso es de libre acceso. Sectigo cuenta con medidas de control de acceso lógico y control de versiones para evitar modificaciones no autorizadas del Repositorio.

2.5. Exactitud de la información

Sectigo, reconociendo su posición de confianza, hace todos los esfuerzos razonables para garantizar que las partes que acceden al Repositorio reciban información precisa, actualizada y

correcta. Sectigo, sin embargo, no puede aceptar ninguna responsabilidad más allá de los límites establecidos en este CP y la póliza de seguro de Sectigo.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

3.1. Nombres

3.1.1. Tipos de nombres

Sectigo emite certificados con DN de sujeto no nulos. Los elementos constitutivos del DN del sujeto se ajustan a ITU X.500.

Sectigo no emite certificados seudónimos excepto como se detalla en la sección **Error! Reference source not found.** de este CP.

Los certificados de autenticación de servidor en general incluyen entradas en la extensión subjectAlternativeName (SAN) que están destinadas a los terceros de confianza.

3.1.2. Necesidad de que los nombres sean significativos

Sectigo coloca nombres significativos en las extensiones de los certificados subjectDN y issuerDN. Los nombres en los certificados identifican al sujeto y al emisor respectivamente.

Los certificados de entidad final contienen nombres significativos con semántica comúnmente entendida que permite la determinación de la identidad del Sujeto del certificado.

El nombre del sujeto en los certificados de la CA debe coincidir con el nombre del emisor en los certificados emitidos por la CA, como lo requiere RFC5280.

3.1.3. Anonimato o seudonimato de los suscriptores.

Sectigo no emite certificados con seudónimos.

3.1.4. Reglas para interpretar varias formas de nombres

Las formas de nombre utilizadas en los DN de sujeto de certificado y DN de emisor se ajustan a un subconjunto de los definidos y documentados en RFC 2253 y UIT-T X.520.

3.1.5. Unicidad de nombres

Sectigo asigna los números de serie de los certificados que aparecen en los certificados de Sectigo. Los números de serie asignados son únicos.

3.1.6. Reconocimiento, autenticación y función de las marcas comerciales

Los suscriptores y solicitantes no pueden solicitar certificados con contenido que infrinja los derechos de propiedad intelectual de otra entidad. A menos que se indique específicamente lo contrario en este CP, Sectigo no verifica el derecho de un solicitante o suscriptor a usar una

marca comercial. Sectigo no resuelve disputas de marcas registradas. Sectigo puede rechazar cualquier solicitud o revocar cualquier certificado que sea parte de una disputa de marca.

Sectigo compara los nombres de los sujetos con un número limitado de marcas comerciales y nombres comerciales que se perciben como de gran valor. Una coincidencia entre una parte del nombre del sujeto y uno de estos nombres de alto valor desencadena un examen más cuidadoso del nombre del sujeto y del solicitante.

3.2. Validación de identidad inicial

Esta sección contiene información sobre los procedimientos de identificación y autenticación de Sectigo para el registro de sujetos como solicitantes, RA, CA y otros participantes. Sectigo podrá utilizar cualquier medio legal de comunicación o investigación para validar la identidad de estos sujetos.

De vez en cuando, Sectigo puede modificar los requisitos relacionados con la información de la aplicación para responder a los requisitos de Sectigo, el contexto comercial del uso de un certificado, otros requisitos de la industria o según lo prescrito por la ley.

3.2.1. Autenticación de la identidad de una persona física

Si el solicitante es una persona física, Sectigo verificará el nombre del solicitante, la dirección del solicitante y la autenticidad de la solicitud de certificado. Las prácticas de verificación se detallan en la CPS.

3.2.2. Autenticación de la identidad de una persona jurídica

Para los certificados de entidad final, la CA verificará la información del sujeto de acuerdo con el reglamento eIDAS y los estándares ETSI. Las prácticas de verificación se detallan en la CPS. Incluidos también los tipos de certificado PSD2.

3.2.3. QWAC

Los certificados QWAC se pueden emitir a personas físicas o jurídicas y siguen los requisitos identificados anteriormente, agregando los del CAB Forum según los BRs y EVGs.

3.2.4. PSD2

Estos certificados se emiten únicamente a personas jurídicas y deberán seguir los mismos requisitos indicados en el apartado 3.2.2 pero al ser emitidos para un sector específico, es necesario especificar y validar información adicional como se explica en la CPS.

3.2.5. Método para demostrar la posesión de la clave privada

Si el solicitante genera el par de claves del certificado, la CA deberá demostrar que el solicitante posee la clave privada. Por lo general, esto se hará verificando la firma digital del solicitante en la Solicitud de firma de certificado (CSR) PKCS # 10 con la clave pública en la CSR.

En el caso de que la generación de claves se realice bajo el control directo de la CA o RA (las emitidas en dispositivos de hardware, es decir, QSCD), no se requiere prueba de posesión.

3.2.6. Validación de autoridad

Antes de emitir certificados a personas jurídicas, Sectigo valida la autoridad del suscriptor para actuar en nombre de la persona jurídica.

3.2.7. Criterios de interoperación

Sectigo puede proporcionar servicios que permitan que otro TSP opere dentro de su PKI o interopere con ella. Dicha interoperación puede incluir certificación cruzada, certificación unilateral u otras formas de operación. Sectigo se reserva el derecho de proporcionar servicios de interoperación y de interoperar de forma transparente con otros TSP; cuyos términos y criterios se establecerán en el acuerdo aplicable.

3.2.8. Validación de la aplicación

Sectigo emplea aplicaciones específicas para validar la identidad del suscriptor. Estos tienen controles específicos que dependen del tipo de certificado.

3.3. Identificación y autenticación para solicitudes de renovación de claves

Sectigo admite cambios de clave en Reemplazo y Renovación. Sectigo requiere que el suscriptor use los mismos detalles de autenticación (generalmente nombre de usuario y contraseña) que usaron en la compra original del certificado. En cualquier caso, si se cambia alguno de los detalles del asunto durante el proceso de reemplazo o renovación, o si los datos de verificación anteriores son más antiguos que el tiempo estipulado para cada tipo de certificado, entonces el asunto debe volver a verificarse.

3.3.1. Identificación y autenticación para el cambio de clave de rutina

La CA y el cambio de clave del certificado del suscriptor siguen los mismos procedimientos que para la emisión del certificado inicial. La identidad puede establecerse mediante el uso de la clave de firma válida actual del dispositivo.

3.3.2. Identificación y autenticación para re-clave después de la revocación

Sectigo no permite de forma rutinaria el cambio de claves (o cualquier forma de Reemplazo o Renovación) después de la revocación. La revocación generalmente se considera un evento terminal en el ciclo de vida del certificado.

En el caso de la revocación del certificado, la emisión de un nuevo certificado generalmente requiere que la parte pase por el proceso de registro inicial según la Sección de CP 3.2.

3.4. Identificación y autenticación para solicitud de revocación

Las solicitudes de revocación deben estar autenticadas. Las solicitudes para revocar un certificado pueden autenticarse utilizando la clave pública de ese certificado, independientemente de si la clave privada asociada se ha visto comprometida.

Revocación a solicitud del suscriptor:

El suscriptor debe estar en posesión de los detalles de autenticación (generalmente nombre de usuario y contraseña) que se utilizaron para comprar el certificado originalmente o el suscriptor debe poder enviar un correo electrónico firmado con la clave privada asociada con el certificado.

Revocación a solicitud de la RA:

La RA debe estar en posesión de los detalles de autenticación utilizados para efectuar la solicitud de certificado original a la CA.

Revocación a solicitud de la CA:

Sectigo no revoca certificados a petición de otros TSP. Sectigo puede revocar los certificados de suscriptor por causa justificada, como se establece en la sección **Error! Reference source not found.** de este CP, pero no se requiere identificación y autenticación en estos casos.

Otros procedimientos aceptables para autenticar solicitudes de revocación incluyen:

- Hacer que el suscriptor inicie sesión en su cuenta y revoque sus certificados a través del portal de su cuenta. El suscriptor enviará su solicitud a través de su cuenta en línea.
- Comunicación con el suscriptor proporcionando garantías razonables de que la persona u organización que solicita la revocación es, de hecho, el suscriptor. Dicha comunicación deberá incluir dos o más de los siguientes: confirmación telefónica, fax firmado, correo electrónico firmado, correo postal o servicio de mensajería.
- El representante es el contacto corporativo, administrador, contacto legal o técnico autenticado en la sección 3.2.5 de esta CP.

4. REQUISITOS OPERATIVOS DEL CICLO DE VIDA DEL CERTIFICADO

Esta sección describe el proceso de solicitud del certificado, incluida la información necesaria para realizar y respaldar una solicitud. Además, esta sección describe algunos de los requisitos impuestos a las RA, suscriptores y otros participantes con respecto al ciclo de vida de un certificado.

El período de validez de los certificados de Sectigo varía según el tipo de certificado, pero por lo general, un certificado será válido por 1 año para los QWAC y hasta 5 años para los otros tipos. Sectigo se reserva el derecho de, a su discreción, emitir certificados que pueden caer fuera de estos períodos establecidos.

4.1. Solicitud de certificado

El proceso de solicitud de certificado debe proporcionar información suficiente para:

- Establecer la autorización del solicitante (por parte de la organización que lo emplea o patrocinadora) para obtener un certificado. (según la Sección 3.2.3)

- Establecer y registrar la identidad del solicitante. (según la Sección 3.2.3)
- Específicamente para los QWAC, obtenga la clave pública del solicitante y verifique que el solicitante posea la clave privada para cada certificado requerido. (según la Sección 3.2.1)
- Verifique cualquier función, autorización u otra información del sujeto solicitada para su inclusión en el certificado.

Estos pasos se pueden realizar en cualquier orden que sea conveniente que no comprometa la seguridad, pero todos deben completarse antes de la emisión del certificado.

La CA y / o RA deberán incluir los procesos, procedimientos y requisitos de su proceso de solicitud de certificado en su CPS.

4.1.1. ¿Quién puede enviar una solicitud de certificado?

Un representante autorizado de la CA solicitante deberá presentar una solicitud para un certificado de CA.

El suscriptor, AOR o una RA en nombre del suscriptor deberá presentar una solicitud de certificado de suscriptor a la CA. Se pueden enviar varias solicitudes de certificado de una RA o AOR como un lote.

4.1.2. Proceso de inscripción y responsabilidades

Todas las comunicaciones entre las CA que respaldan la solicitud de certificado y el proceso de emisión deberán estar autenticadas y protegidas contra modificaciones; Se protegerá cualquier transmisión electrónica de secretos compartidos e información de identificación personal. Las comunicaciones pueden ser electrónicas o fuera de banda. Cuando se utilicen comunicaciones electrónicas, se utilizarán mecanismos criptográficos acordes. Las comunicaciones fuera de banda protegerán la confidencialidad e integridad de los datos.

Los solicitantes son responsables de proporcionar información precisa sobre sus solicitudes de certificado.

El proceso de inscripción, para un solicitante, incluye lo siguiente:

- Completar la solicitud del certificado
- Proporcionar la información solicitada
- Responder a las solicitudes de autenticación de manera oportuna
- Envío del pago requerido, cuando corresponda

4.2. Procesamiento de solicitud del certificado

La información contenida en las solicitudes de certificados debe verificarse como precisa antes de que se emitan los certificados. Los procedimientos para verificar la información en las solicitudes de certificados se especifican en la CPS.

4.2.1. Realización de funciones de identificación y autenticación

La identificación y autenticación del suscriptor deberá cumplir con los requisitos especificados para la autenticación del suscriptor como se especifica en las Secciones 3.2 y 3.3. Los componentes de la PKI (por ejemplo, CA o RA) que son responsables de autenticar la identidad del suscriptor en cada caso.

4.2.2. Aprobación o rechazo de solicitudes de certificados

Cualquier solicitud de certificado que sea recibida por Sectigo bajo esta política, para la cual se haya validado la identidad y autorización del solicitante, será debidamente procesada. Sin embargo, Sectigo rechazará cualquier solicitud para la que no se pueda completar dicha validación, o cuando Sectigo tenga motivos para no confiar en la solicitud o el proceso de certificación.

Sectigo se reserva el derecho de rechazar una solicitud para emitir un certificado a un solicitante si, en la opinión exclusiva de Sectigo, al emitir un certificado a dicho solicitante, el nombre de Sectigo podría verse empañado, disminuido su valor, etc. y bajo tales circunstancias pueden hacerlo sin incurrir en responsabilidad alguna por cualquier pérdida o gasto que surja como resultado de dicha negativa.

Un solicitante cuya solicitud haya sido rechazada puede volver a presentarla posteriormente.

En todos los tipos de certificados cualificados de Sectigo, el suscriptor tiene la obligación continua de monitorear la precisión de la información enviada y notificar a Sectigo de cualquier cambio que pueda afectar la validez del certificado. El incumplimiento de las obligaciones establecidas en el Acuerdo de Suscriptor resultará en la revocación del certificado del suscriptor sin previo aviso al suscriptor y el suscriptor deberá pagar cualquier cargo pero que aún no se haya pagado en virtud del Acuerdo de Suscriptor.

4.2.3. Procesar las solicitudes de certificados

Sectigo realiza esfuerzos razonables para confirmar la información de la solicitud de certificado y emitir un certificado dentro de un período razonable. El período depende en gran medida del tipo de certificado y los requisitos de verificación establecidos en la CPS.

De vez en cuando, eventos fuera del control de Sectigo pueden retrasar el proceso de emisión; sin embargo, Sectigo hará todos los esfuerzos razonables para cumplir con los tiempos de emisión y para informar a los solicitantes de cualquier factor que pueda afectar los tiempos de emisión de manera oportuna.

4.2.4. Autorización de la autoridad de certificación

Cuando una solicitud es para un certificado que incluye un nombre de dominio y se va a utilizar para la autenticación del servidor, que es el caso de los QWAC, Sectigo examina los registros de recursos de DNS de autorización de la autoridad de certificación (CAA) según se especifica en RFC 6844 enmendado por la errata 5065 (Apéndice A) y, si dichos Registros CAA están presentes y no otorgan a Sectigo la autoridad para emitir el certificado, la solicitud es rechazada.

Cuando las etiquetas 'issue' y 'issuewild' están presentes dentro de un registro CAA, Sectigo reconoce los siguientes nombres de dominio dentro de esas etiquetas como autorización para su emisión:

- sectigo.com
- usertrust.com
- trust-provider.com

Durante un período de transición, Sectigo reconoce los siguientes nombres de dominio que otorgan autorización, aunque están obsoletos y deben reemplazarse por un nombre de dominio de la lista anterior lo antes posible.

- comodo.com
- comodoca.com

4.3. Emisión de certificados

4.3.1. Acciones de la CA durante la emisión del certificado

Al recibir la solicitud, las CA / RA deberán:

- Verificar la identidad del solicitante como se especifica en la Sección 3.2.
- Verificar la autoridad del solicitante y la integridad de la información en la solicitud de certificado como se especifica en la Sección 4.1.
- Crear y firmar un certificado si se han cumplido todos los requisitos del certificado (en el caso de una RA, hacer que la CA firme el certificado).
- Poner el certificado a disposición del suscriptor después de confirmar que el suscriptor ha reconocido formalmente sus obligaciones como se describe en la Sección 9.6.3.

Los sistemas automatizados de Sectigo reciben y recopilan:

- Evidencia recopilada durante el proceso de verificación, y / o
- Afirman que la verificación se ha completado de acuerdo con la política y la documentación interna que establece los medios aceptables para verificar la información del sujeto.

Los sistemas automatizados de Sectigo registran los detalles de la transacción comercial asociada con el envío de una solicitud de certificado y la eventual emisión de un certificado.

Los sistemas automatizados (y manuales) de Sectigo registran la fuente de, y todos los detalles enviados con, evidencia de verificación, que han sido realizados por RA externos o por la RA interna de Sectigo.

Se requiere la autenticación correcta de la evidencia de verificación proporcionada por las RA externas antes de que esa evidencia se considere para la emisión del certificado.

4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado

Las CA que operan bajo esta política informarán al suscriptor (u otro sujeto del certificado) de la creación de un certificado y pondrán el certificado a disposición del suscriptor. Para los certificados de dispositivo, la CA deberá emitir el certificado de acuerdo con el protocolo de solicitud de certificado utilizado por el dispositivo (esto puede ser automatizado) y, si el protocolo no proporciona una notificación inherente, también notificará al representante de la organización autorizado de la emisión (esto puede ser en lote).

4.3.3. Negarse a emitir un certificado

Sectigo se reserva el derecho de negarse a emitir un certificado a cualquier parte como lo considere oportuno, sin incurrir en responsabilidad alguna por cualquier pérdida o gasto que surja de dicha negativa. Sectigo se reserva el derecho de no revelar las razones de tal negativa.

4.4. Aceptación del certificado

Esta sección describe algunas de las acciones del suscriptor al aceptar un certificado. Además, describe cómo Sectigo publica un certificado y cómo Sectigo notifica a otras entidades sobre la emisión de un certificado.

Antes de que un suscriptor pueda hacer un uso efectivo de su clave privada, la CA deberá explicar al suscriptor sus responsabilidades y obtener el reconocimiento del suscriptor, como se define en la Sección 9.6.3.

4.4.1. Conducta que constituye la aceptación del certificado

La siguiente conducta constituye la aceptación del certificado por parte del suscriptor:

- Usando el certificado
- No objetar el certificado o su contenido dentro de los 30 días posteriores a su emisión

4.4.2. Publicación del certificado por la CA

Como se especifica en la Sección 2.1, todos los certificados emitidos por la CA se publican en repositorios.

Un certificado se publica a través de varios medios: (1) por Sectigo haciendo que el certificado esté disponible en el Repositorio; y (2) por el suscriptor que usa el certificado posterior a la entrega del certificado por parte de Sectigo.

4.4.3. Notificación de la emisión del certificado por parte de la CA a otras entidades

Se debe notificar a la Autoridad de Políticas cada vez que una CA que opera bajo esta política emita un certificado de CA.

Las RA pueden recibir notificación de la emisión de certificados que aprueban.

Los certificados QWAC también se publican en registros CT de conformidad con las políticas de BR, EVG y / o los root programs de los navegadores.

4.5. Par de claves y uso de certificados

4.5.1. Uso de certificado y clave privada del suscriptor

El alcance de uso previsto para una clave privada se especificará a través de extensiones de certificado, incluido el uso de clave y las extensiones de uso de clave extendido, en el certificado asociado.

4.5.2. Uso de certificado y clave pública del tercero de confianza

La decisión final sobre si confiar en una firma o sello electrónico verificado es exclusivamente del tercero confía. Los certificados pueden especificar restricciones de uso a través de extensiones de certificado críticas, incluidas las restricciones básicas y extensiones de uso de claves. Todas las CA que operan bajo esta política deben emitir CRL que especifiquen el estado de todos los certificados vigentes, excepto los certificados de respuesta OCSP. Se recomienda que las partes que confían procesen y cumplan con esta información siempre que utilicen certificados en una transacción.

4.6. Renovación del certificado

Renovación del certificado significa la emisión de un nuevo certificado al suscriptor sin cambiar la clave pública del suscriptor u otro participante o cualquier otra información en el certificado.

4.6.1. Circunstancia para la renovación del certificado

La renovación del certificado de entidad final puede ser compatible con certificados en los que la clave privada asociada con el certificado no se ha visto comprometida. Los certificados de entidad final pueden renovarse para mantener la continuidad del uso del certificado.

Un certificado de entidad final puede renovarse después de su vencimiento. El certificado original puede o no ser revocado, pero no se volverá a cambiar la clave, se renovará ni se modificará.

4.6.2. Quién puede solicitar la renovación

El suscriptor, RA o AOR pueden solicitar la renovación de un certificado de suscriptor.

4.6.3. Procesamiento de solicitudes de renovación de certificados

Para una solicitud de renovación de certificado, se confirmará la identidad del solicitante de acuerdo con los requisitos especificados en la Sección 3.2.

4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor

Según la Sección 4.3.2.

4.6.5. Conducta que constituye la aceptación de un certificado de renovación

Según la Sección 4.4.1.

4.6.6. Publicación del certificado de renovación por parte de la CA

Según la Sección 4.4.2.

4.6.7. Notificación de la emisión del certificado por parte de la CA a otras entidades

Según la Sección 4.4.3

4.7. Cambio de clave del certificado

La renovación de la clave de un certificado consiste en crear nuevos certificados con una clave pública diferente (y un número de serie y un identificador de clave) mientras se conserva el contenido restante del certificado anterior que describe el asunto. Al nuevo certificado se le puede asignar un período de validez diferente, especificar un punto de distribución de CRL diferente y / o estar firmado con una clave diferente. La nueva clave de un certificado no requiere un cambio en el subjectName.

Un certificado antiguo puede o no ser revocado, pero no se volverá a cambiar la clave, se renovará ni se modificará.

4.7.1. Circunstancia para el cambio de clave del certificado

Cuanto más tiempo y más a menudo se utiliza una clave, más susceptible es a la pérdida o al descubrimiento. Por lo tanto, es importante que un suscriptor obtenga periódicamente nuevas claves. (La Sección 6.3.2 establece períodos de uso de claves privadas para CA y suscriptores). Ejemplos de circunstancias que requieren una nueva clave del certificado incluyen: vencimiento, pérdida o compromiso, emisión de un nuevo token de hardware y fallo del token de hardware.

4.7.2. Quién puede solicitar la certificación de una nueva clave pública

Aquellos que pueden solicitar un cambio de clave de certificado incluyen, entre otros, el suscriptor, el RA en nombre del suscriptor o Sectigo a su discreción.

4.7.3. Procesamiento de solicitudes de cambio de claves de certificados

Para el cambio de clave del certificado, la CA deberá confirmar la identidad del suscriptor de acuerdo con los requisitos especificados en la Sección 3.2 para la autenticación de una Solicitud de certificado original.

La nueva clave del certificado de CA debe ser aprobada por la Autoridad de Políticas.

4.7.4. Notificación de la emisión de un nuevo certificado al suscriptor

Según la Sección 4.3.2.

4.7.5. Conducta que constituye la aceptación de un certificado con clave nueva

Según la Sección 4.4.1.

4.7.6. Publicación del certificado con nueva clave por parte de la CA

Según la Sección 4.4.2.

4.7.7. Notificación de la emisión del certificado por parte de la CA a otras entidades

Según la Sección 4.4.3.

4.8. Modificación del certificado

Sectigo no ofrece modificación de certificados. En cambio, Sectigo revocará el certificado anterior y emitirá un nuevo certificado como reemplazo.

4.9. Revocación y suspensión de certificados

Las CA que operan bajo esta política pueden emitir CRL y deben proporcionar respuestas OCSP que cubran todos los certificados no vencidos emitidos bajo esta política, excepto el respondedor OCSP.

Sectigo no utiliza la suspensión de certificados.

4.9.1. Circunstancias para la revocación

Un certificado se revocará cuando la vinculación entre el sujeto y la clave pública del sujeto definida en el certificado ya no se considere válida. Cuando esto ocurra, el certificado asociado se revocará y se colocará en la CRL y / o se agregará al respondedor OCSP. Los certificados revocados se incluirán en todas las publicaciones nuevas de la información sobre el estado del certificado hasta que expiren.

Las CA que operan bajo esta política deberán revocar un certificado dentro de las 24 horas siguientes si ocurre una o más de las siguientes situaciones:

- El suscriptor solicita por escrito que la CA revoque el certificado;
- El suscriptor notifica a la CA que la solicitud de certificado original no fue autorizada y no otorga autorización retroactivamente;
- La CA obtiene evidencia de que la Clave Privada del suscriptor correspondiente a la Clave Pública en el certificado sufrió un Compromiso de Clave;
- Específicamente para los QWAC, la CA obtiene evidencia de que no se debe confiar en la validación de la autorización de dominio o el control de cualquier Nombre de dominio completo o dirección IP en el certificado.

Las CA que operan bajo esta política deben revocar un certificado dentro de las 24 horas y en 5 días si ocurre una o más de las siguientes situaciones:

- El certificado ya no cumple con los requisitos de las Secciones 6.1.5 y 6.1.6;
- La CA obtiene evidencia de que el certificado se usó indebidamente;
- La CA es consciente de que un suscriptor ha violado una o más de sus obligaciones materiales bajo el Acuerdo de Suscriptor o los Términos de Uso;

- Específicamente para los QWAC, la CA es consciente de cualquier circunstancia que indique que el uso de un nombre de dominio totalmente calificado o una dirección IP en el certificado ya no está permitido legalmente (por ejemplo, un tribunal ha revocado el derecho de un registrante de nombre de dominio a usar el dominio).
- Específicamente para los QWAC, la CA es consciente de que se ha utilizado un certificado comodín para autenticar un nombre de dominio completo subordinado engañoso;
- Se informa a la CA de un cambio sustancial en la información contenida en el certificado;
- La CA es consciente de que el certificado no se emitió de acuerdo con estos Requisitos o la Política de certificados de la CA o la Declaración de Prácticas de Certificación;
- La CA determina o tiene conocimiento de que la información que aparece en el certificado es inexacta;
- El derecho de la CA a emitir certificados bajo estos Requisitos expira o se revoca o termina, a menos que la CA haya hecho arreglos para continuar manteniendo el Repositorio CRL / OCSP;
- La revocación es requerida por la Política de certificados de la CA y / o la Declaración de prácticas de certificación; o
- La CA es consciente de un método demostrado o comprobado que expone la clave privada del suscriptor a un compromiso, se han desarrollado métodos que pueden calcularla fácilmente en función de la clave pública (como una clave débil de Debian, consultar http://wiki.debian.org/SSLkeys), o si hay evidencia clara de que el método específico utilizado para generar la clave privada era defectuoso.

Sectigo también puede revocar un certificado si ocurre cualquiera de las siguientes situaciones:

- Las obligaciones del suscriptor o de Sectigo bajo este CP o el Acuerdo de Suscriptor correspondiente se retrasan o evitan por un desastre natural, fallo en los ordenadores o de las comunicaciones, u otra causa fuera del control razonable de la persona y, como resultado, la información de otra persona está materialmente amenazada o comprometida;
- Ha habido una modificación de la información perteneciente al suscriptor que está contenida en el certificado;
- Un número de identificación personal, clave privada o contraseña tiene, o es probable que sea conocido por alguien no autorizado para usarlo, o se está usando o es probable que se use de manera no autorizada;
- No se ha emitido un certificado digital de suscriptor de acuerdo con las políticas establecidas en esta CP;
- El suscriptor ha utilizado el Servicio de Suscripción en contra de la ley, regla o regulación, o Sectigo cree razonablemente que el suscriptor está usando el certificado, directa o indirectamente, para participar en actividades ilegales o fraudulentas;
- El certificado se expidió a personas físicas o jurídicas identificadas como editores de software malintencionado o que se hiciera pasar por otras personas físicas o jurídicas;
- El certificado fue emitido como resultado de fraude o negligencia; o

- El certificado, si no se revoca, comprometerá el estado de confianza de Sectigo.

Sectigo revocará un certificado de CA subordinada dentro de los siete (7) días si ocurre una o más de las siguientes situaciones:

- La CA subordinada solicita la revocación por escrito;
- La CA subordinada notifica a Sectigo que la solicitud de certificado original no fue autorizada y no otorga la autorización retroactivamente;
- Sectigo obtiene evidencia de que la Clave Privada de la CA Subordinada correspondiente a la Clave Pública en el certificado sufrió un Compromiso de Clave;
- Sectigo obtiene evidencia de que el certificado de la CA subordinada se usó indebidamente;
- Sectigo tiene conocimiento de que el certificado de la CA subordinada no se emitió de acuerdo con, o que la CA subordinada no ha cumplido con este CP;
- Sectigo determina que la información que aparece en el certificado de la CA subordinada es inexacta o engañosa;
- Sectigo o la CA subordinada cesan sus operaciones por cualquier motivo y no han hecho arreglos para que otra CA proporcione soporte de revocación para el certificado;
- El derecho de Sectigo, o la CA subordinada, de emitir certificados expira o se revoca o cancela, a menos que Sectigo haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;
- Esta CP requiere la revocación;
- La CA subordinada ha utilizado el certificado en contra de la ley, norma o reglamento, o Sectigo cree razonablemente que la CA subordinada está utilizando el certificado, directa o indirectamente, para participar en actividades ilegales o fraudulentas;
- El certificado de la CA subordinada fue emitido a personas físicas o jurídicas identificadas como editores de software malicioso o que se hizo pasar por otras personas o entidades;
- El certificado de la CA subordinada fue emitido como resultado de fraude o negligencia;
- El certificado de la CA subordinada, si no se revoca, comprometerá el estado de confianza de Sectigo.

4.9.2. Quién puede solicitar la revocación

Las solicitudes de revocación pueden ser realizadas por:

- El suscriptor del certificado o cualquier representante autorizado del suscriptor
- La CA o RA afiliada
- La autoridad política

Otras partes pueden reportar sospechas de Compromiso de la Clave Privada, uso indebido de certificados u otros tipos de fraude, compromiso, conducta inapropiada o cualquier otro asunto relacionado con los certificados, en primera instancia, por correo electrónico a qcabuse@sectigo.com.

4.9.3. Procedimiento de solicitud de revocación

Sectigo acepta y responde a solicitudes de revocación e informes de problemas las 24 horas del día, los 7 días de la semana. Antes de la revocación de un certificado, Sectigo verificará que la solicitud de revocación haya sido:

- Realizado por la persona física o jurídica que ha realizado la solicitud del certificado.
- Realizado por la RA en nombre de la persona física o jurídica que utilizó la RA para realizar la solicitud del certificado, y
- Ha sido autenticado por los procedimientos de la Sección 3.4 de este CP.

4.9.4. Tiempo dentro del cual la CA debe procesar la solicitud de revocación

Sectigo procesará las solicitudes de revocación de acuerdo con este documento. Una vez que se ha revocado un certificado, la revocación se reflejará en las respuestas OCSP emitidas en 1 hora y en las CRL en 6 horas.

4.9.5. Requisito de verificación de revocación para los terceros de confianza

El uso de certificados revocados podría tener consecuencias catastróficas o perjudiciales en determinadas aplicaciones. La cuestión de la frecuencia con la que se deben obtener nuevos datos de revocación es una determinación que debe realizar el tercero que confía. Si es temporalmente inviable obtener información de revocación, entonces el tercero de confianza debe rechazar el uso del certificado o tomar una decisión informada para aceptar el riesgo, la responsabilidad y las consecuencias de usar un certificado cuya autenticidad no puede garantizarse según los estándares de esta CP.

Depender de una firma o sello electrónico no verificable puede resultar en riesgos que el tercero, y no Sectigo, asume en su totalidad.

Por medio de este CP, Sectigo ha informado adecuadamente a las partes confiantes sobre el uso y validación de firmas o sellos electrónicos a través de este CP y otra documentación publicada en el Repositorio o contactando a través de medios fuera de banda a través de la dirección de contacto como se especifica en el Control de Documentos.

4.9.6. Frecuencia de emisión de CRL (si corresponde)

Para el estado de los certificados de suscriptor:

Si la CA publica una CRL, la CA deberá actualizar y volver a emitir las CRL al menos una vez cada 24 horas.

Para conocer el estado de los certificados de la CA:

La CA deberá actualizar y volver a emitir las CRL al menos (i) una vez cada doce meses (ii) dentro de las 24 horas posteriores a la revocación de un certificado de CA subordinada, y el valor del campo nextUpdate no debe exceder los doce meses del valor del campo thisUpdate (iii) dentro de las 24 horas posteriores a la expiración de un certificado de CA

4.9.7. Latencia máxima para las CRL (si corresponde)

Cada CRL se publicará a más tardar a la hora especificada en el campo nextUpdate de la CRL emitida anteriormente para el mismo alcance.

4.9.8. Disponibilidad de verificación del estado / revocación en línea

Las respuestas OCSP cumplen con RFC6960 y / o RFC5019. Las respuestas OCSP deben:

1. Estar firmadas por la CA que emitió los certificados cuyo estado de revocación se está verificando, o
2. Estar firmadas por un respondedor OCSP cuyo certificado esté firmado por la CA que emitió el certificado cuyo estado de revocación se está verificando.

En el último caso, el certificado de firma OCSP debe contener una extensión de tipo id-pkix-ocsp-nocheck, como se define en RFC6960.

4.9.9. Requisitos de verificación de revocación en línea

Todas las CA que operan bajo este CP admiten una capacidad OCSP utilizando el método GET para certificados emitidos de acuerdo con estos Requisitos.

Para el estado de los certificados de suscriptor:

Las CA que operan bajo esta política deberán actualizar la información proporcionada a través de OCSP al menos cada cuatro días. Las respuestas OCSP de este servicio tienen un tiempo máximo de vencimiento de diez días.

Para conocer el estado de los certificados de CA subordinada:

- Sectigo actualizará la información proporcionada a través de un Protocolo de estado de certificado en línea (OCSP) al menos (i) cada doce meses (ii) dentro de las 24 horas posteriores a la revocación de un certificado de CA subordinada (iii) dentro de las 24 horas posteriores a la expiración de un certificado de CA subordinada

Si el respondedor OCSP recibe una solicitud de estado de un certificado que no ha sido emitido, entonces el respondedor no debe responder con un estado "bueno". Sectigo debe monitorear al respondedor para tales solicitudes como parte de sus procedimientos de respuesta de seguridad.

4.10. Servicios del estado de los certificados

4.10.1. Características operativas

Las entradas de revocación en una CRL o Respuesta OCSP están disponibles más allá del período de validez del certificado.

4.10.2. Servicio disponible

Los servicios de estado de certificados están disponibles 24 horas al día, 7 días a la semana. Los servicios CRL y OCSP se operan y mantienen con recursos suficientes para proporcionar un tiempo de respuesta de diez segundos o menos en condiciones normales de funcionamiento.

4.11. Fin de suscripción

Se especifica en la CPS y / o Acuerdo de Suscriptor.

5. CONTROLES OPERATIVOS, DE GESTIÓN Y DE INSTALACIONES

Todo el equipo de CA y RA está protegido contra robo, pérdida y acceso no autorizado en todo momento. Está prohibido el uso no autorizado de equipos CA y RA. El equipo de CA se dedica a realizar funciones de CA. El equipo de RA se operará para garantizar que el equipo cumpla con todos los controles físicos en todo momento.

5.1. Controles físicos

Todos los sistemas de CA están protegidos contra el acceso no autorizado. El TSP implementa controles de acceso físicos para reducir el riesgo de alteración del equipo. Todos los sistemas de CA están protegidos contra robo, pérdida y uso no autorizado.

Todos los requisitos de control físico que se especifican a continuación se aplican igualmente a las CA raíz y secundaria, y a cualquier estación de trabajo remota utilizada para administrar las CA, excepto donde se indique específicamente.

5.1.1. Ubicación y construcción del sitio o CPD

Todos los sistemas de CA están ubicados dentro de un entorno protegido físicamente que disuade, previene y detecta el uso, el acceso o la divulgación no autorizados de información y sistemas sensibles. La ubicación y construcción de la instalación que alberga el equipo de CA, así como los sitios que albergan estaciones de trabajo remotas que se utilizan para administrar la CA, son consistentes con las instalaciones que se utilizan para albergar información sensible de alto valor. La ubicación y la construcción del CPD, cuando se combinan con otros mecanismos de protección de seguridad física, como guardias, cerraduras de alta seguridad y sensores de intrusión, proporcionarán una protección sólida contra el acceso no autorizado a los equipos y registros de CA.

Dichos entornos se basan en parte en el establecimiento de niveles de seguridad física. Un nivel es una barrera, como una puerta cerrada con llave o una puerta cerrada, que proporciona control de acceso obligatorio para las personas y requiere una respuesta positiva (por ejemplo, la puerta se abre o la puerta se cierra) para que cada individuo pase a la siguiente área. Cada nivel sucesivo proporciona un acceso más restringido y una mayor seguridad física contra intrusiones o accesos no autorizados. Además, cada nivel de seguridad física encapsula el siguiente nivel interior, de modo que un nivel interior debe estar completamente contenido en un nivel exterior y no puede tener una pared exterior común con el nivel exterior, siendo el

nivel más exterior la barrera exterior del edificio (p. Ej., una cerca perimetral o una pared exterior).

El TSP deberá construir o diseñar las instalaciones que albergan sus funciones de CA con al menos cuatro niveles de seguridad física. Los TSP realizarán todas las operaciones de validación dentro del Nivel 2 o superior. Sectigo coloca los sistemas de servicios de información necesarios para respaldar las funciones de CA en el nivel 4 o superior. Los módulos criptográficos en línea y fuera de línea se colocan en el Nivel 4 o superior. Los TSP protegerán aún más los módulos criptográficos fuera de línea colocándolos dentro del Nivel 4 o superior cuando no estén en uso.

La ubicación y construcción del sitio se describe con más detalle en la CPS.

5.1.2. Acceso físico

5.1.2.1. Acceso físico para equipos de la CA

El acceso a cada nivel de seguridad física, construido de acuerdo con la sección 5.1.1 del CP, debe ser auditable y controlado de modo que solo el personal autorizado pueda acceder a cada nivel.

Existen sistemas de acceso con tarjeta para controlar y monitorear el acceso a todas las áreas de la instalación. El acceso a la maquinaria física 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 monitoreadas por personal de seguridad, personal de recepción o sistemas de monitoreo / control.

5.1.2.2. Acceso físico para equipos de RA

El equipo RA está protegido contra el acceso no autorizado mientras el módulo criptográfico RA está instalado y activado. La RA implementará controles de acceso físicos para reducir el riesgo de alteración del equipo incluso cuando el módulo criptográfico no esté instalado y activado. Estos mecanismos de seguridad son proporcionales al nivel de amenaza en el entorno del equipo de RA.

5.1.3. Energía y aire acondicionado

Las instalaciones de CA están equipadas con sistemas de energía primaria y de respaldo para garantizar un acceso continuo e ininterrumpido a la energía eléctrica. Además, estas instalaciones están equipadas con sistemas de calefacción / ventilación / aire acondicionado primarios y de respaldo para el control de la temperatura.

Las instalaciones de CA tienen la capacidad de respaldo suficiente para bloquear la entrada, finalizar cualquier acción pendiente y registrar el estado del equipo automáticamente antes de que la falta de energía o el aire acondicionado provoque un apagado. Los repositorios (que contienen certificados de CA y CRL) cuentan con energía ininterrumpida suficiente para un mínimo de seis (6) horas de operación en ausencia de energía, para mantener la disponibilidad y evitar la denegación de servicio.

5.1.4. Exposiciones al agua

Las instalaciones de Sectigo se construyen, equipan e instalan, y se implementan procedimientos, para evitar inundaciones u otra exposición dañina al agua. Los daños potenciales por agua de las medidas de prevención y protección contra incendios (por ejemplo, sistemas de rociadores/extintores) están excluidos de este requisito.

5.1.5. Prevención y protección contra incendios

Las instalaciones de Sectigo están construidas y equipadas, y se implementan procedimientos, para prevenir y extinguir incendios u otra exposición dañina a llamas o humo. Estas medidas cumplen con todas las normas de seguridad locales aplicables.

5.1.6. Almacén de datos

Los medios de Sectigo se almacenan para protegerlos de daños accidentales (por ejemplo, agua, fuego o electromagnéticos) y el acceso físico no autorizado. Los medios que contienen información de auditoría, archivo o copia de seguridad se duplican y almacenan en una ubicación separada de la ubicación de la CA.

Los medios que contengan material de clave privada se manipularán, empaquetarán y almacenarán de manera que cumpla con los requisitos del nivel de confidencialidad de la información que protege o a la que proporciona acceso. La protección del almacenamiento de material de clave privada de la CA y RA es coherente con las estipulaciones de la Sección 5.1.2.

5.1.7. Deposito de basura

El personal de CA y de operaciones y el personal de RA deberán eliminar y destruir los desechos normales de la oficina de acuerdo con la política local. Los medios utilizados para recopilar o transmitir información de privacidad serán destruidos, de modo que la información sea irrecuperable, antes de su eliminación. Los medios y el papel sensibles se destruyen de acuerdo con la política aplicable para la destrucción de dicho material.

La destrucción de medios y documentación que contengan información confidencial, como material de clave privada, deberá emplear métodos acordes con los de la Publicación especial 800-88 del NIST.

5.1.8. Copia de seguridad fuera del sitio

Sectigo respalda su información en ubicaciones seguras fuera del sitio que están lo suficientemente distantes entre sí para escapar de los daños potenciales de un desastre en la ubicación principal que afecta a una ubicación de respaldo.

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. La copia de seguridad del software de CA crítico se realiza semanalmente y se almacena fuera del sitio. La copia de seguridad de la información empresarial crítica se realiza a diario y se almacena fuera del sitio. El acceso a los servidores / medios de respaldo está restringido únicamente al personal autorizado. Los medios de copia de seguridad se prueban periódicamente a través de

la restauración para garantizar que se pueda confiar en ellos en caso de desastre. Los servidores / medios de respaldo están etiquetados apropiadamente de acuerdo con la sensibilidad de la información.

Los requisitos para la copia de seguridad de la clave privada de CA se especifican en la Sección 6.2.4.

5.2. Controles de procedimiento

5.2.1. Roles confiables

Los roles de confianza son asignados por miembros superiores del equipo de gestión que asignan permisos sobre la base del "principio de privilegio mínimo" a través de un proceso de autorización formal con las autorizaciones archivadas.

La lista de personal designado para funciones de confianza se mantiene y revisa anualmente.

Las funciones y deberes realizados por personas en roles de confianza se distribuyen de modo que una sola persona no pueda subvertir la seguridad y la confiabilidad de las operaciones de PKI. Todo el personal en funciones de confianza está libre de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones de la PKI de Sectigo.

Las personas que actúan en roles de confianza solo pueden acceder a un Sistema de gestión de certificados (CMS) después de que se hayan autenticado mediante un método aprobado como adecuado para el control.

5.2.1.1. Administradores de la CA

El administrador de la CA instala y configura el software de la CA, incluida la generación de claves y la copia de seguridad de claves (como parte de la generación de claves) y la recuperación posterior.

Los administradores de la CA no emiten certificados a los suscriptores.

5.2.1.2. Oficiales de la CA (por ejemplo, CMS, RA, personal de validación y verificación)

El rol de Oficial de la CA es responsable de emitir y revocar certificados, la verificación de identidad y el cumplimiento de los pasos de emisión requeridos, incluidos los definidos en este CP y el registro de los detalles de los pasos de aprobación y emisión realizados, y las tareas de verificación de identidad.

Los oficiales de la CA deben identificarse y autenticarse a sí mismos en los sistemas antes de que se otorgue el acceso. La identificación se realiza a través de un nombre de usuario, y la autenticación requiere una contraseña y un certificado.

5.2.1.3. Operador (por ejemplo, administradores de sistemas / ingenieros de sistemas)

Los operadores instalan y configuran el hardware del sistema, incluidos servidores, enrutadores, firewalls y redes. El operador también mantiene actualizados los sistemas CA,

CMS y RA con parches de software y otro mantenimiento necesario para la estabilidad, seguridad y recuperación del sistema.

5.2.1.4. Auditores internos

Los auditores internos son responsables de revisar, mantener y archivar los registros de auditoría y realizar o supervisar las auditorías de cumplimiento interno para determinar si Sectigo, una CA externa o RA está operando de acuerdo con este CP y, cuando sea relevante, un contrato de RA.

5.2.1.5. Personal de RA

El personal de la RA son las personas que desempeñan funciones de confianza que operan y gestionan los componentes de la RA.

5.2.2. Número de personas necesarias por tarea

Los procedimientos de control de múltiples partes están diseñados para garantizar que, como mínimo, el número deseado de personas de confianza esté presente para obtener acceso físico o lógico al equipo de la CA. El acceso a los módulos criptográficos de la CA se hace cumplir estrictamente por varias personas de confianza a lo largo de su ciclo de vida, desde la recepción y la inspección de entrada hasta la destrucción lógica y / o física final. Una vez que se activa una CA con claves operativas, se invocarán más controles de acceso para mantener el control dividido sobre el acceso físico y lógico a la CA.

Sectigo requiere que al menos dos administradores de CA para:

- Acceso físico
- Generación de claves de la CA;
- Activación de la clave de firma de la CA; y
- Copia de seguridad y restauración de la clave privada de la CA

Cuando se requiera el control de varias partes, al menos uno de los participantes es un administrador. Todos los participantes deben desempeñar un rol de confianza como se define en la Sección 5.2.2. El control de múltiples partes no se logrará utilizando personal que se desempeñe en el rol de confianza de los auditores internos.

5.2.3. Identificación y autenticación para cada rol

Sectigo confirma la identidad y autorización de todo el personal que busca convertirse en Personas de confianza antes de que dicho personal sea:

- Dispositivos de acceso emitidos y acceso concedido a las instalaciones requeridas;
- Contar con credenciales electrónicas para acceder y realizar funciones específicas en los sistemas de la CA.

La autenticación de la identidad incluye la presencia personal (física) de dicho personal ante Personas de confianza que desempeñan funciones de recursos humanos o de seguridad dentro de una entidad y una verificación de formas de identificación reconocidas, como pasaportes,

identificaciones nacionales y licencias de conducir. La identidad se confirmará mediante los procedimientos de verificación de antecedentes de la Sección 5.3.

5.3. Controles de personal

5.3.1. Requisitos de calificaciones, experiencia y autorización

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

Todas las personas que desempeñan funciones de confianza se seleccionan en función de su lealtad, confiabilidad e integridad, y están sujetas a una investigación de antecedentes. El personal designado para funciones de confianza deberá:

- Poseer el conocimiento experto, la experiencia y las calificaciones necesarias para los servicios ofrecidos y la función laboral adecuada;
- Haber completado con éxito un programa de formación adecuado;
- Haber demostrado capacidad para desempeñar sus funciones;
- Ser confiable;
- No tener otros deberes que interfieran o entren en conflicto con sus deberes para el rol de confianza;
- No haber sido relevado previamente de sus funciones por negligencia o incumplimiento de sus funciones;
- No haber sido condenado por un delito grave u otro delito que afecte su idoneidad para el puesto; y
- Haber sido designado por escrito por la dirección de la CA.

El rol de operador solo se otorga en los sistemas de TI de Sectigo cuando existe una necesidad comercial específica. Los nuevos operadores no reciben todos los derechos de administrador hasta que hayan demostrado un conocimiento detallado de los sistemas y políticas de TI de Sectigo y que hayan alcanzado un nivel de habilidad adecuado satisfactorio para el administrador de sistemas o el director ejecutivo. Los nuevos administradores son supervisados de cerca por el Administrador de sistemas durante los primeros tres meses. Cuando los sistemas lo permiten, la autenticación de acceso del administrador se realiza a través de una clave pública / privada emitida específicamente para este propósito. Esto proporciona responsabilidad a los administradores individuales y permite monitorear sus actividades.

Al rol de oficial de CA se le otorgan privilegios de emisión de certificados solo después de una capacitación suficiente en las políticas y procedimientos de validación y verificación de Sectigo.

5.3.2. 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, etc.

5.3.3. Requisitos de formación

Sectigo proporciona una formación adecuada a todo el personal antes de que asuman un rol de confianza en caso de que aún no tengan el conjunto de habilidades completo requerido para ese rol. 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.

La capacitación se llevará a cabo en las siguientes áreas:

- Principios y mecanismos de seguridad de la CA o RA;
- Todas las versiones de software PKI en uso en el sistema de la CA o RA;
- Todas las tareas de PKI que se espera que realicen;
- Informes y manejo de incidentes y compromisos
- Procedimientos de recuperación de desastres y continuidad comercial; y
- Estipulaciones de esta CP.

Los administradores y operadores de CA están capacitados en el mantenimiento, la configuración y el uso del software, los sistemas operativos y los sistemas de hardware específicos que utiliza Sectigo. Los auditores internos están capacitados para dominar los principios generales de auditoría de sistemas y procesos, así como familiarizarse con las políticas y procedimientos de Sectigo. Los funcionarios de CA están capacitados en las políticas y procedimientos de validación y verificación de Sectigo.

5.3.4. Frecuencia de formación

Sectigo brinda formación de actualización a su personal en la medida y frecuencia requeridas para garantizar que dicho personal mantenga el nivel de competencia requerido para desempeñar sus responsabilidades laborales de manera competente y satisfactoria.

Todas las personas responsables de las funciones de PKI deben conocer los cambios en la operación de la CA. Cualquier cambio significativo en las operaciones cuenta con un plan de formación (concienciación) y la ejecución de dicho plan está documentada. Ejemplos de tales cambios son la actualización de software o hardware de la CA, cambios en los sistemas de seguridad automatizados y reubicación de equipos.

Se mantiene la documentación que identifica a todo el personal que recibió la formación y el nivel de formación completado.

5.3.5. 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 medidas disciplinarias que pueden incluir el despido. Si las acciones no autorizadas de cualquier persona revelan un

fallo o deficiencia en la capacitación, se ofrecerá formación suficiente para rectificar la deficiencia.

5.3.6. Requisitos del contratista independiente

Sectigo permitirá que los contratistas o consultores independientes se conviertan en Personas de confianza solo en la medida necesaria para dar cabida a relaciones de subcontratación claramente definidas. El TSP solo debe utilizar contratistas o consultores como personas de confianza si la CA no tiene empleados adecuados disponibles para desempeñar las funciones de personas de confianza. Los contratistas y consultores independientes son acompañados y supervisados directamente por personas de confianza cuando se les da acceso a la CA y sus instalaciones seguras.

Los contratistas que cumplen funciones de confianza están sujetos a todos los requisitos de personal estipulados en esta política y deberán establecer procedimientos para garantizar que los subcontratistas se desempeñen de acuerdo con esta política.

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

5.3.7. Documentación suministrada al personal

Sectigo brinda a su personal la formación y la documentación necesarias para desempeñar sus responsabilidades laborales de manera competente y satisfactoria.

5.4. Procedimientos de registro de auditoría

Para fines de auditoría, Sectigo mantiene registros electrónicos de los siguientes eventos para las funciones principales.

5.4.1. Tipos de eventos registrados

Se mantiene un registro de auditoría de cada movimiento de los medios extraíbles.

Eventos de gestión del ciclo de vida de certificados:

- Funciones clave de firma de la CA Raíz, incluida la generación, copia de seguridad, recuperación y destrucción de claves
- Gestión del ciclo de vida de los certificados del suscriptor, incluidas las solicitudes de certificados satisfactorias y no satisfactorias, las emisiones de certificados, las reemisiones de certificados y las renovaciones de certificados
- Solicitudes de revocación de certificados de suscriptor, incluido el motivo de la revocación
- Cambios de afiliación del suscriptor que invalidarían la validez de un certificado existente
- Actualizaciones, generaciones y emisiones de CRL
- Custodia de claves y de dispositivos y soportes de claves

- Clave privada comprometida

Eventos relacionados con la seguridad:

- Tiempo de inactividad del sistema, fallos de software y fallos de hardware
- Acciones del sistema de la CA realizadas por el personal de Sectigo, incluidas actualizaciones de software, reemplazos de hardware y actualizaciones
- Eventos criptográficos del HSM, como uso, desinstalación, servicio o reparación y retiro
- Intentos de acceso a la PKI de Sectigo exitosos y fallidos
- Entrada y salida segura de las instalaciones de la CA

Información de la solicitud de certificado:

- La documentación y otra información relacionada presentada por el solicitante como parte del proceso de validación de la solicitud.
- Ubicaciones de almacenamiento, ya sean físicas o electrónicas, de los documentos presentados

Todos los registros incluyen los siguientes elementos:

- Fecha y hora de entrada
- Método de entrada
- Fuente de entrada
- Identidad de la entidad que realiza la entrada del registro

5.4.2. Registro de frecuencia de procesamiento

El administrador del sistema archiva semanalmente los registros y diarios de eventos que la administración de la CA revisa semanalmente.

5.4.3. Período de retención del registro de auditoría

Los registros de auditoría se conservan durante al menos 7 años y deben conservarse de la manera que se describe a continuación. Para la RA, un administrador del sistema que no sea la RA es responsable de administrar el registro de auditoría.

5.4.4. Protección del registro de auditoría

Solo los administradores de la CA tienen el nivel de acceso del sistema necesario para modificar o eliminar registros.

Tanto los registros actuales como los archivados se mantienen en una forma que evita la modificación, sustitución o destrucción no autorizadas.

5.4.5. Procedimientos de copia de seguridad del registro de auditoría

Todos los registros se copian a diario y se archivan semanalmente en una ubicación externa.

5.4.6. Sistema de realización de auditorías (interno vs. externo)

Los procesos automáticos de recopilación de auditorías se ejecutan desde el inicio del sistema hasta el apagado del sistema. El fallo de un sistema de auditoría automatizado que pueda afectar negativamente la integridad del sistema o la confidencialidad de la información protegida por el sistema llevará a los Operadores de Sectigo y / o Administradores de la CA a evaluar si se requiere una suspensión de las operaciones hasta que se solucione el problema.

5.4.7. Evaluaciones de vulnerabilidad

Una vulnerabilidad es una debilidad en la organización o en un sistema de información que puede ser aprovechada por una amenaza, con la posibilidad de causar daño a los activos. Con el fin de mitigar el riesgo o la posibilidad de causar daños a los activos, Sectigo realiza evaluaciones de vulnerabilidad periódicas con un enfoque doble. Sectigo evalúa las vulnerabilidades (1) haciendo una evaluación de las amenazas, impactos y vulnerabilidades de los activos y la probabilidad de que ocurran, y (2) desarrollando un proceso de selección e implementación de controles de seguridad para reducir los riesgos. identificado en la evaluación de riesgos a un nivel aceptable. Sectigo realiza evaluaciones de vulnerabilidad de forma rutinaria identificando las categorías de vulnerabilidad a las que se enfrenta un activo. Algunas de las categorías de vulnerabilidad que evalúa Sectigo son técnicas, lógicas, humanas, etc.

Sectigo emplea a terceros para realizar análisis de vulnerabilidades y pruebas de penetración regulares en nuestros sistemas / infraestructura de la CA.

5.5. Archivo de registros

Sectigo implementa un estándar de archivo para todos los sistemas críticos para el negocio ubicados en sus centros de datos. Sectigo conserva registros en formatos electrónicos o en papel de conformidad con esta subsección de este CP.

5.5.1. Tipos de registros archivados

Sectigo realiza una copia de seguridad de los datos de la aplicación y del sistema. Sectigo puede archivar la siguiente información:

- Datos de auditoría, como se especifica en la sección 5.4 de este CP;
- Información de la solicitud de certificado;
- Documentación que respalde una solicitud de certificado;
- Información del ciclo de vida del certificado.

5.5.2. Periodo de conservación del archivo

El período de retención de la información archivada depende del tipo de información, el nivel de confidencialidad de la información y el tipo de sistema en el que se almacena la información.

Sectigo conserva los registros de los certificados de Sectigo y la documentación asociada por un período no menor a 15 años, o según sea necesario para cumplir con las leyes aplicables. El plazo de retención comienza en la fecha de vencimiento o revocación. Se conservan copias de

los certificados, independientemente de su estado (como vencidos o revocados). Dichos registros pueden conservarse en formato electrónico, en papel o en cualquier otro formato que Sectigo considere oportuno.

Los datos del usuario respaldados desde una estación de trabajo se conservan durante un período mínimo de 6 meses.

5.5.3. Protección del archivo

Los registros se archivan en una ubicación segura fuera del sitio o DPC y se mantienen en una forma que evita la modificación, sustitución o destrucción no autorizadas. El acceso a servidores de respaldo y / o medios de respaldo, ya sea Windows o Linux, utilidades de respaldo o datos de respaldo, está restringido solo al personal autorizado y se adhiere a una estricta política de denegación predeterminada.

5.5.4. Procedimientos de respaldo de archivos

La información electrónica se respaldará de manera incremental a diario y se realizarán respaldos completos semanalmente.

Los administradores de cada ubicación de Sectigo son responsables de realizar y mantener las actividades de respaldo. Sectigo emplea copias de seguridad programadas y no programadas. Las copias de seguridad programadas se automatizan mediante herramientas de copia de seguridad aprobadas. Las copias de seguridad programadas se controlan mediante herramientas automatizadas. Las copias de seguridad no programadas ocurren antes de realizar cambios importantes en los sistemas críticos y son parte de cualquier solicitud de cambio que tenga un posible impacto en la integridad o seguridad de los datos. Todos los medios de respaldo están etiquetados de acuerdo con la clasificación de la información, que se basa en la información de respaldo almacenada en los medios.

5.5.5. Requisitos para el sellado de tiempo de los registros

Los registros de archivo de la CA se sellan automáticamente a medida que se crean. Los relojes del sistema utilizados para el sellado de tiempo se mantienen en sincronía con un estándar de tiempo autorizado. La CPS describe cómo los relojes del sistema utilizados para el sellado de tiempo se mantienen en sincronía con un estándar de tiempo autorizado.

Los registros con sello de tiempo incluyen, entre otros, los siguientes:

- Entrada de visitantes,
- Salida de visitante,
- Correos electrónicos dentro de Sectigo,
- Correos electrónicos enviados entre Sectigo y terceros,
- Acuerdos de suscriptor,
- Emisión de certificados y
- Revocación de certificado.

5.5.6. Sistema de recolección de archivos (interno o externo)

El sistema de recopilación de archivos de Sectigo es tanto interno como externo. Como parte de sus procedimientos internos de recopilación, Sectigo puede requerir que los suscriptores envíen la documentación adecuada para respaldar una solicitud de certificado.

Como parte de los procedimientos de recopilación externos de Sectigo, los RA pueden requerir documentación de los suscriptores para admitir aplicaciones de certificados, en su función de Sectigo RA. En tales circunstancias, los RA están obligados a conservar dichos registros de acuerdo con las prácticas de conservación y protección de registros utilizadas por Sectigo y según lo establecido en este CP.

5.5.7. Procedimientos para obtener y verificar información de archivo

Los procedimientos, que detallan cómo crear, verificar, empaquetar, transmitir y almacenar la información del Archivo, se describen en la CPS correspondiente.

5.6. Cambio de clave

Hacia el final de la vida útil de cada clave privada, se encarga un nuevo par de claves de firma de la CA. Cuando se cambia la clave de un certificado de la CA, solo se usa la nueva clave para firmar certificados a partir de ese momento. Si la antigua clave privada se utiliza para firmar los certificados de respuesta OCSP o las CRL que cubren los certificados firmados con esa clave, la antigua clave se conservará y protegerá. El nuevo certificado de clave pública de la CA correspondiente se proporciona a los suscriptores y terceros de confianza a través de los métodos de entrega detallados en la CPS.

5.7. Compromiso y recuperación ante desastres

Las organizaciones se enfrentan regularmente a eventos que pueden interrumpir sus actividades comerciales normales o pueden conducir a la pérdida de información y activos. Estos eventos pueden ser el resultado de desastres naturales, accidentes, fallos de equipos o acciones deliberadas. Esta sección detalla los procedimientos que emplea Sectigo en caso de un compromiso o desastre.

5.7.1. Procedimientos de manejo de incidentes y compromisos

Todos los incidentes, tanto presuntos como reales, se informan a la autoridad correspondiente para su investigación. Dependiendo de la naturaleza y la inmediatez del incidente, el informante de un incidente debe documentar los detalles del incidente para ayudar con la evaluación del incidente, la investigación, la solución y los cambios operativos futuros. Una vez que se informa el incidente, la autoridad competente realiza una evaluación inicial. A continuación, se elige e implementa una estrategia de contención. Una vez que se ha contenido un incidente, es necesaria la erradicación para eliminar los componentes del incidente. Durante la erradicación, se le da importancia a identificar todas las áreas afectadas para que puedan ser remediadas.

Estos procedimientos están en su lugar para asegurar que

- una respuesta consistente a los incidentes que ocurren en los activos de Sectigo,
- los incidentes se detectan, notifican y registran, y
- Se definen roles y responsabilidades claros.

Para mantener la integridad de sus servicios, Sectigo implementa, documenta y prueba periódicamente los planes y procedimientos apropiados de recuperación ante desastres y contingencias. Estos procedimientos definen y contienen un proceso formal de reporte de gestión de incidentes, respuesta a incidentes y procedimientos de escalado de incidentes para garantizar la gestión profesional de incidentes y el regreso a las operaciones normales de manera oportuna. El proceso también permite analizar las incidencias de manera que se identifiquen las posibles causas, de modo que se mejoren las debilidades en los procesos de Sectigo para evitar que vuelvan a ocurrir. Dichos planes se revisan y actualizan al menos una vez al año.

5.7.2. Los recursos informáticos, el software y / o los datos están dañados

Si Sectigo determina que sus recursos informáticos, software u operaciones de datos se han visto comprometidos, Sectigo investigará el alcance del compromiso y el riesgo presentado a las partes afectadas. Dependiendo del alcance del compromiso, Sectigo se reserva el derecho de revocar los certificados afectados, revocar claves de entidad, proporcionar nuevas claves públicas a los usuarios y recertificar sujetos.

5.7.3. Procedimientos de compromiso de clave privada de la CA

Debido a la naturaleza de las claves privadas de CA, estas se clasifican como muy críticas para las operaciones comerciales y la continuidad de Sectigo. Si alguna de las claves de firma privadas de la CA se vio comprometida o se sospecha que está comprometida, Sectigo realizaría una evaluación para determinar la naturaleza y el alcance del compromiso. En las circunstancias más graves, Sectigo revocaría todos los certificados emitidos por el uso de esas claves, notificaría a todos los propietarios de certificados (por correo electrónico) de esa revocación y ofrecería volver a emitir los certificados a los clientes con una alternativa o una nueva calve privada de firma.

5.7.4. Procedimientos de compromiso de algoritmos

Sectigo verifica todos los algoritmos utilizados en sus sistemas y sigue las mejores prácticas y estándares de la industria, por ejemplo, ETSI TS 119 312.

5.7.5. Capacidades de continuidad empresarial después de un desastre

Sectigo opera un sistema CA 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 CA de respaldo está disponible en caso de que la CA principal deje de funcionar. Todo el equipo informático crítico de Sectigo está alojado en instalaciones de coubicación administradas por proveedores de centros de datos comerciales independientes, 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 CA 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 facilidades para administrar el ciclo de vida de un certificado, incluyendo pero no limitado a la aplicación, emisión, revocación y renovación de dichos certificados. Además de un sistema de CA completamente redundante, Sectigo mantiene disposiciones para la activación de una CA de respaldo en 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 CA.

5.8. Terminación del TSP

En caso de finalización de las operaciones del TSP por cualquier motivo, Sectigo proporcionará un aviso oportuno y la transferencia de responsabilidades a las entidades sucesoras, el mantenimiento de registros y las reparaciones. Antes de terminar sus propias actividades como TSP, Sectigo tomará los siguientes pasos, cuando sea posible:

- Proporcionar a los suscriptores de certificados válidos con noventa (90) días de anticipación de su intención de dejar de actuar como TSP.
- Revocar todos los certificados que aún no hayan sido revocados o vencidos al final del período de notificación de noventa (90) días sin solicitar el consentimiento del suscriptor.
- Dar aviso oportuno de la revocación a cada suscriptor afectado.
- Hacer arreglos razonables para preservar sus registros de acuerdo con este CP.
- Se reserva el derecho de proporcionar acuerdos de sucesión para la reemisión de certificados por un TSP sucesor que tenga todos los permisos pertinentes para hacerlo y cumpla con todas las reglas necesarias, mientras que su operación es al menos tan segura como la de Sectigo.

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

6. CONTROLES DE SEGURIDAD TÉCNICA

6.1. Generación e instalación de pares de claves

6.1.1. Generación de pares de claves

La generación de pares de claves de suscriptor se describe en la CPS.

La generación de pares de claves de la CA debe realizarse utilizando módulos y procesos criptográficos validados por lo menos según FIPS 140-2 Nivel 3 que proporcionen la solidez criptográfica requerida de las claves generadas y eviten la pérdida, divulgación, modificación o uso no autorizado de claves privadas. Todos los números aleatorios utilizados junto con los

parámetros para el material de generación de claves se generarán mediante un método aprobado por FIPS.

Las claves de la CA se generan en una ceremonia de generación de claves como se especifica en la CPS.

La generación de pares de claves de la CA crea una pista de auditoría verificable indicando de que se siguieron los requisitos de seguridad según los procedimientos. La documentación del procedimiento debe ser lo suficientemente detallada para demostrar que se utilizó la separación de roles adecuada. Un tercero independiente validará la ejecución de los procedimientos de generación de claves, ya sea presenciando la generación de claves o examinando el video, el registro firmado o documentado de la generación de claves.

6.1.2. Entrega de clave privada al suscriptor

El suscriptor o CA deberá realizar la generación de pares de claves de suscriptor. Si los propios suscriptores generan claves privadas, la entrega de claves privadas a un suscriptor es innecesaria.

Cuando las CA generan pares de claves en nombre del suscriptor, la clave privada se entrega de forma segura al suscriptor. Las claves privadas se entregan electrónicamente o en un módulo criptográfico de hardware certificado por FIPS o QSCD. En todos los casos, deberán cumplirse los siguientes requisitos:

- Excepto en los casos en que Sectigo opera un servicio de archivo de claves en nombre del suscriptor, la CA no retendrá ninguna copia de la clave durante más de dos semanas después de la entrega de la clave privada al suscriptor.
- Las CA utilizarán sistemas certificados por FIPS o QSCD y entregarán claves privadas a los suscriptores a través de SSL / TLS y asegurarán dicha entrega mediante el uso de un paquete PKCS # 8 o, a discreción exclusiva de las CA, cualquier otro medio comparablemente equivalente (por ejemplo, PKCS # 12) para evitar la pérdida, divulgación, modificación o uso no autorizado de dichas claves privadas.
- Cuando los pares de claves se generen previamente en tokens de hardware, las entidades que distribuyan dichos tokens harán todo lo posible para proporcionar seguridad física de los tokens para evitar la pérdida, divulgación, modificación o uso no autorizado de las claves privadas en ellos. La RA mantendrá un registro del acuse de recibo del suscriptor del token.
- El suscriptor acusará recibo de la (s) clave (s) privada (s).
- La entrega se realizará de una manera que garantice que se proporcionen los tokens y los datos de activación correctos a los suscriptores correctos.
    - Para los módulos de hardware, la responsabilidad por la ubicación y el estado del módulo se mantendrá hasta que el suscriptor acepte su posesión.
    - Para la entrega electrónica de claves privadas, el material de la clave se cifrará utilizando un algoritmo criptográfico y un tamaño de clave al menos tan fuerte

como la clave privada. Los datos de activación se entregarán mediante un canal seguro separado.

6.1.3. Entrega de clave pública al emisor del certificado

Cuando se transfiere una Clave Pública a la CA emisora para ser certificada, se entrega a través de un mecanismo que valida la identidad del suscriptor y asegura que la Clave Pública no ha sido alterada durante el tránsito y que el solicitante del certificado posee la Clave Privada correspondiente a la Clave pública transferida. El solicitante del certificado deberá entregar la clave pública en un PKCS # 10 CSR o un método equivalente que asegure que la clave pública no ha sido alterada durante el tránsito; y el solicitante del certificado posee la Clave Privada correspondiente a la Clave Pública transferida. El solicitante del certificado enviará el CSR a Sectigo según el método aprobado.

6.1.4. Entrega de clave pública de la CA a los terceros de confianza

La clave pública de una CA raiz se proporciona a los terceros que confían de forma segura para que no sea vulnerable a modificaciones o sustituciones. Los métodos aceptables para la entrega incluyen, entre otros:

- Cargar una CA raiz en los tokens entregados a los terceros de confianza a través de mecanismos seguros;
- Distribución segura a través de mecanismos seguros fuera de banda;
- Comparación del hash del certificado (huella dactilar) con el hash de la CA raiz disponible a través de fuentes fuera de banda autenticadas (hay que tener en cuenta que las huellas dactilares o hash publicados junto con el certificado no son aceptables como mecanismo de autenticación); y
- Descargar una CA raiz de sitios web de confianza (por ejemplo, un sitio web de CA) asegurado con un certificado válido actualmente de igual o mayor nivel de seguridad que el certificado que se descarga y esa CA raiz no está en la cadena de certificados para el certificado del sitio web.

Los sistemas que utilizan tokens de hardware criptográficos almacenan certificados de confianza de modo que la alteración o sustitución no autorizada sea fácilmente detectable.

6.1.5. Tamaños de clave

Este CP requiere el uso de firmas RSA PKCS # 1, RSASSA-PSS, DSA o ECDSA; Las restricciones adicionales sobre los tamaños de clave y los algoritmos hash se detallan a continuación. Los certificados emitidos bajo esta política deben contener RSA o claves públicas de curva elíptica.

Todos los certificados que vencen el 31 de diciembre de 2030 o antes deben contener claves públicas de sujeto de al menos 2048 bits para RSA / DSA, al menos 256 bits para curva elíptica y estar firmados con la clave privada correspondiente.

Todos los certificados que vencen después del 31 de diciembre de 2030 deben contener claves públicas de sujeto de al menos 3072 bits para RSA / DSA, al menos 256 bits para curva elíptica y estar firmados con la clave privada correspondiente.

Las CA que generan certificados y CRL bajo esta política deben usar el algoritmo hash SHA-256 o SHA-384 al generar firmas digitales.

Las firmas ECDSA en certificados y CRL deben generarse utilizando SHA-256 o SHA-384, según corresponda para la longitud de la clave.

Las firmas RSA en las CRL que solo proporcionan información de estado para los certificados que se generaron con SHA-1 pueden seguir generándose con SHA-1.

Cuando se implementen, los CSS firmarán las respuestas utilizando el mismo algoritmo de firma, tamaño de clave y algoritmo hash que utiliza la CA para firmar las CRL.

6.1.6. Generación de parámetros de clave pública y control de calidad

Sectigo genera los parámetros de clave pública. Las claves de la CA de Sectigo se generarán dentro de un HSM certificado con certificación FIPS 140-2 Nivel 3 o QSCD.

6.1.7. Propósitos de uso clave

El uso de una clave específica está restringido por la extensión keyUsage en el certificado X.509.

Las claves públicas vinculadas a los certificados de CA se utilizan para firmar certificados e información de estado (por ejemplo, CRL). La siguiente tabla muestra la configuración específica de la extensión keyUsage para los certificados de CA y especifica que todos los certificados de la CA (es decir, CA raíz, CA secundaria):

- Deberá incluir una extensión de clave
- Establecerá la criticidad de la extensión keyUsage en TRUE
- Deberá afirmar el bit digitalSignature, el bit keyCertSign y el bit cRLSign en la extensión de uso de la clave

Tabla: extensión keyUsage para todos los certificados de CA

Campo	Formato	Criticidad	Valor	Comentario
keyUsage	BIT STRING	CIERTO	{id-ce 15}	Incluido en todos los certificados de CA
firma digital	(0)		0	obligatorio
no repudio	(1)		0	No establecido
claveEncipherment	(2)		0	No establecido
cifrado de datos	(3)		0	No establecido

keyAgreement	(4)		0	No establecido
keyCertSign	(5)		1	Obligatorio
cRLSign	(6)		1	Obligatorio
cifrarOnly	(7)		0	No establecido
descifrar	(8)		0	No establecido

La configuración específica de la extensión keyUsage para los certificados de entidad final se especificará en la CPS.

6.2. Protección de clave privada y controles del módulo criptográfico

6.2.1. Estándares y controles de módulos criptográficos

Las claves privadas de la CA dentro de esta PKI están protegidas mediante sistemas FIPS 140-2 de nivel 3 o se enumeran como QSCD. Los titulares de claves privadas tomarán las precauciones necesarias para evitar la pérdida, divulgación, modificación o uso no autorizado de dichas claves privadas de acuerdo con este CP y cualquier obligación contractual existente.

6.2.2. Transferencia de clave privada hacia o desde un módulo criptográfico

Cuando las claves de firma de la CA Raiz se respaldan en otro módulo de seguridad de hardware criptográfico, dichas claves se transfieren entre dispositivos bajo control de varias personas y solo en formato cifrado.

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.

6.2.4. Método de activación de la clave privada

Todas las CA protegen los datos de activación de sus claves privadas contra pérdida, robo, modificación, divulgación o uso no autorizado.

Los administradores de la CA se autentican en el token criptográfico antes de la activación de las claves privadas asociadas. Los medios aceptables de autenticación incluyen, entre otros, frases de contraseña, PIN o datos biométricos. La entrada de datos de activación está protegida contra la divulgación (es decir, los datos no deben mostrarse mientras se introducen).

Para los certificados de dispositivo, el dispositivo puede configurarse para activar su clave privada, siempre que se implementen los controles de acceso físicos y lógicos apropiados para el dispositivo. La fuerza de los controles de seguridad será proporcional al nivel de amenaza en el entorno del

dispositivo y protegerá el hardware, el software, las claves privadas y sus datos de activación del dispositivo contra cualquier compromiso.

6.2.4.1. Activación del administrador de la CA

El método de activación del sistema de la CA por parte de un administrador de la CA requiere:

- Utilizar una tarjeta inteligente, un Dispositivo de acceso biométrico, una contraseña de acuerdo con la Sección 6.4.1 o un sistema de seguridad equivalente para autenticar al administrador antes de la activación de la clave privada, que incluye, por ejemplo, una contraseña para operar la clave privada, una Contraseña de inicio de sesión de Windows o protector de pantalla, o una contraseña de inicio de sesión de red; y
- Tomar medidas comercialmente razonables para la protección física de la estación de trabajo del administrador para evitar el uso de la estación de trabajo y su clave privada asociada sin la autorización del administrador.

6.2.4.2. Clave privada de la CA offline

Una vez que se ha activado el sistema de CA, se requiere un número límite de personas para proporcionar sus datos de activación para activar una clave privada de la CA offline, como se define en la Sección 6.2.2. Una vez activada la Clave Privada, estará activa hasta la terminación de la sesión.

6.2.4.3. Claves privadas de la CA online

Las claves privadas de una CA online se activan mediante un número umbral de personas, según se define en la Sección 6.2.2, que proporcionan sus datos de activación (almacenados en medios seguros). Una vez que se activa la clave privada, la clave privada puede estar activa por un período indefinido hasta que se desactive cuando la CA se desconecte.

6.2.4.4. Claves privadas del dispositivo

Un dispositivo puede configurarse para activar su clave privada, siempre que se implementen los controles de acceso físicos y lógicos adecuados para el dispositivo. Los controles de seguridad serán proporcionales al nivel de amenaza en el entorno del Dispositivo y protegerá el hardware, el software, las Claves privadas y sus datos de activación del Dispositivo contra cualquier compromiso. Si la clave privada se almacena de forma protegida mediante cifrado basado en contraseña, entonces se deben introducir los datos de activación de la contraseña o frase de contraseña cada vez que se inicializan el dispositivo y la aplicación de seguridad para desbloquear la clave privada para uso operativo.

6.2.5. Método para desactivar la clave privada

Los módulos criptográficos que se hayan activado no estarán disponibles para el acceso no autorizado. Después de su uso, el módulo criptográfico se desactiva, por ejemplo, mediante un procedimiento de cierre de sesión manual o automáticamente después de un período de inactividad. Los módulos criptográficos de la CA se almacenan de forma segura cuando no se utilizan.

Cuando una CA online se desconecta, el token que contiene la clave privada se elimina del lector para desactivarlo.

Con respecto a las Claves Privadas de las CA offline, después de la finalización de una Ceremonia de Generación de Claves, en la que dichas Claves Privadas se utilizan para operaciones de Claves Privadas, el token que contiene las Claves Privadas se retira del lector para desactivarlas. Una vez retirados del lector, los tokens se almacenan de forma segura.

Cuando se desactivan, las claves privadas se mantienen cifradas únicamente. Se borran de la memoria antes de que se desasigne la memoria. Cualquier espacio en disco donde se almacenaron las claves privadas se sobrescribe antes de que el espacio se libere al sistema operativo.

6.2.6. Método de destrucción de la clave privada

Destruir una clave privada significa la destrucción de todas las claves activas, tanto respaldadas como almacenadas. La destrucción de una clave privada comprenderá eliminarla del HSM y eliminarla del conjunto de respaldo activo. Las claves privadas se destruyen de acuerdo con NIST SP 800-88.

6.2.7. Clasificación del módulo criptográfico

Consulte la sección 6.2.1.

6.3. Otros aspectos de la gestión de los pares de claves

6.3.1. Archivo de clave pública

La clave pública se archiva como parte del archivo del certificado. La CA emisora retiene todas las claves públicas de verificación durante un mínimo de 15 años o según lo requiera la ley aplicable o la regulación de la industria.

6.3.2. Períodos operativos del certificado y períodos de uso de pares de claves

Generalmente, el período de validez del certificado se establecerá de la siguiente manera, sin embargo, Sectigo se reserva el derecho de ofrecer períodos de validez fuera de este estándar.

- Los certificados de CA raíz pueden tener un período de validez de hasta 25 años
- Los certificados Sub-CA pueden tener un período de validez de hasta 15 años

Los certificados cualificados de entidad final pueden tener un período de validez de hasta 5 años. Los períodos de validez están anidados de manera que los períodos de validez de los certificados emitidos están incluidos dentro del período de validez de la CA emisora.

6.4. Datos de activación

Los datos de activación se refieren a valores de datos distintos de las claves privadas completas que se requieren para operar claves privadas o módulos criptográficos que contienen claves privadas. Los ejemplos de datos de activación incluyen, entre otros, PIN, frases de contraseña y partes de claves privadas utilizadas en un régimen de división de claves.

6.4.1. Generación e instalación de datos de activación

Los datos de activación se generan de acuerdo con las especificaciones del HSM.

6.4.2. Protección de datos de activación

Los procedimientos utilizados para proteger los datos de activación dependen de si los datos son para tarjetas inteligentes o contraseñas. El personal de gran confianza tiene tarjetas inteligentes. Las contraseñas y las tarjetas inteligentes están sujetas a la Política criptográfica de Sectigo.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Sectigo asegura la integridad de sus sistemas informáticos mediante la implementación de controles, tales como:

- Aplicar los mismos controles de seguridad a todos los sistemas ubicados en la misma zona con un sistema certificado;
- Mantenimiento de sistemas de CA online en una zona de alta seguridad
- Mantener las CA raíz separadas de otras redes;
- Mantener y proteger los sistemas de emisión, los sistemas de gestión de certificados y los sistemas de soporte de seguridad;
- Configurar sistemas de emisión, sistemas de gestión de certificados, sistemas de soporte de seguridad y sistemas de soporte interno / front-end eliminando o deshabilitando todas las cuentas, aplicaciones, servicios, protocolos y puertos que no se utilizan en las operaciones de Sectigo y permitiendo solo aquellos que están aprobados por Sectigo;
- Revisar las configuraciones de los sistemas de emisión, los sistemas de gestión de certificados, los sistemas de soporte de seguridad y los sistemas de soporte interno / front-end semanalmente;
- Someterse a pruebas de penetración de forma periódica y después de actualizaciones importantes de la infraestructura o las aplicaciones;
- Otorgar acceso de administración a los Sistemas de Certificación solo a personas que actúen en roles confiables y requieran su responsabilidad por la seguridad del Sistema de Certificación; y
- Cambiar las claves de autenticación y las contraseñas para cualquier cuenta privilegiada o cuenta de servicio en un Sistema de Certificación siempre que se cambie o revoque la autorización de una persona para acceder administrativamente a esa cuenta en el Sistema de Certificación.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo del sistema

Sectigo cuenta con políticas formales para controlar, documentar y monitorear el desarrollo de sus sistemas de CA. Las solicitudes de desarrollo solo pueden ser presentadas por un grupo

restringido de personal. Las tareas de desarrollo son priorizadas por los 'solicitantes de tareas' dentro de su área y luego el gerente de desarrollo las prioriza aún más mientras se considera la lista de tareas de desarrollo en su totalidad. Sectigo desarrolla la mayoría de los cambios internamente. En el caso de que Sectigo 'compre' servicios (hardware y / o software), los proveedores se seleccionan en función de la reputación y la capacidad de suministrar productos 'adecuados para su propósito'.

Al recibir cada solicitud de desarrollo, se asignan un ID de tarea y un título único que permanecen con la tarea durante todo el ciclo de vida del desarrollo.

Cada tarea de desarrollo tiene una evaluación de riesgos asociada que se lleva a cabo como parte del ciclo de vida del desarrollo. Se considera que todas las tareas conllevan algún tipo de riesgo, desde cuestiones relacionadas con el alcance y la complejidad de la tarea hasta la falta de disponibilidad de recursos. La gestión de riesgos se aborda a través de un proceso formal de gestión de riesgos y la solicitud no se aplica al entorno de producción hasta que se logre un nivel de riesgo aceptable.

El producto de trabajo de todas las solicitudes de desarrollo se somete a una revisión por pares antes de su lanzamiento al entorno de producción para evitar que se cargue software malicioso o erróneo en el entorno de producción.

El equipo de control de calidad prueba y aprueba cada tarea antes de implementarla en el entorno de producción. Los desarrolladores no pueden participar en la prueba de su propio trabajo. Cuando QA encuentra problemas, el equipo de QA proporciona comentarios al desarrollador para resolverlos antes de que el desarrollo pueda proceder a la publicación.

Los miembros del equipo de desarrollo y control de calidad no tienen acceso al entorno de producción. El acceso a estas áreas está estrictamente controlado.

Una vez que el cambio se ha implementado en el entorno de producción, se informa al solicitante de la tarea junto con el equipo de pruebas y se vuelve a probar el cambio.

6.6.2. Controles de gestión de seguridad

Sectigo tiene herramientas y procedimientos para garantizar que los sistemas operativos y las aplicaciones de Sectigo conserven su integridad y permanezcan configurados de forma segura. Estas herramientas y procedimientos incluyen la verificación de la integridad de la aplicación y el software de seguridad.

6.7. Controles de 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 los sistemas de certificados en redes o zonas en función de su relación funcional, lógica y física;

- Aplicar los mismos controles de seguridad a todos los sistemas ubicados en la misma zona con un Sistema de Certificación;
- 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 protegen los sistemas y las comunicaciones entre los sistemas dentro de zonas seguras y las comunicaciones con sistemas que no son certificados 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 los sistemas de certificados, implementación de controles de detección y prevención para protegerse contra virus y software malicioso; y
- Cambiar las claves de autenticación y las contraseñas para cualquier cuenta privilegiada o cuenta de servicio en un Sistema de Certificación siempre que se cambie o revoque la autorización de una persona para acceder administrativamente a esa cuenta en el Sistema de Certificación.

6.8. Sellado de tiempo

Todos los componentes de la CA se sincronizan regularmente con un servicio horario como el reloj atómico del Instituto Nacional de Estándares y Tecnología (NIST) o el Servicio de Protocolo de Tiempo de Red NIST. La hora derivada del servicio horario se utiliza para establecer la hora de:

- Tipo de validez inicial del certificado de un dispositivo;
- Revocación del certificado de un dispositivo;
- Publicación de actualizaciones de CRL; y
- OCSP u otras respuestas de la CA.

Los certificados, las CRL y otras entradas de la base de datos de revocación contienen información de fecha y hora. Se pueden utilizar procedimientos electrónicos o manuales para mantener la hora del sistema. Los ajustes del reloj son eventos auditables (consulte la Sección 5.4.1).

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

7.1. Perfil de certificado

Los certificados cumplen con RFC 5280 y RFC6818: certificado de infraestructura de clave pública X.509 de Internet y perfil de lista de revocación de certificados (CRL), mayo de 2008 y actualizaciones del certificado de infraestructura de clave pública X.509 de Internet y perfil de lista de revocación de certificados (CRL), enero de 2013 Los campos de texto se codifican utilizando la codificación printableString siempre que sea posible y la codificación utf8String si es necesario.

Los certificados contienen la identidad y los datos de atributos de un sujeto que utiliza el certificado base con las extensiones aplicables. El certificado base contiene el número de versión del certificado, el número de serie de identificación del certificado, el algoritmo de firma utilizado para firmar el certificado, el nombre distinguido del emisor, el período de validez del certificado, el nombre distinguido del sujeto, información sobre la clave pública del sujeto, y extensiones como se define en el documento de Perfiles de Certificados eIDAS de Sectigo o la CPS.

Las CA que operan bajo esta política generarán números de serie de certificados no secuenciales mayores que cero (0) que contengan al menos 64 bits de salida de un CSPRNG.

7.1.1. Número (s) de versión

Los certificados de Sectigo son certificados X.509 v3. El número de versión del certificado se establece en el valor entero de "2" para los certificados de la Versión 3.

7.1.2. Extensiones de certificado

Como se describe en el documento Perfiles de certificados eIDAS de Sectigo o en la CPS.

7.1.3. Identificadores de objetos de algoritmo

Los certificados de Sectigo se firman mediante algoritmos que incluyen, entre otros, RSA y ECDSA. Se pueden encontrar detalles adicionales en el documento Sectigo eIDAS Certificate Profiles o en el CPS.

7.1.4. Formas de nombres

Como se especifica en la Sección 3.1.1.

7.1.5. Identificador de objeto de política de certificado

Como se especifica en el documento Perfiles de certificados eIDAS de Sectigo o en la CPS.

7.1.6. Sintaxis y semántica de los policy qualifiers

Un uso común de los calificadores de políticas es proporcionar información de ubicación (por ejemplo, URI) para una política de certificado. Si esto es deseable, el uso se especificará en el documento Perfiles de certificados eIDAS de Sectigo o en la CPS.

7.2. Perfil de CRL

Sectigo gestiona y pone a disposición del público directorios de certificados revocados mediante CRL. Todas las CRL emitidas por Sectigo son CRL X.509v2, en particular como se perfilan en RFC5280. Se recomienda encarecidamente a los usuarios y las partes que confían que consulten los directorios de certificados revocados en todo momento antes de confiar en la información incluida en un certificado. Sectigo actualiza y publica una nueva CRL cada 24 horas o con mayor frecuencia en circunstancias especiales. La CRL para cualquier certificado emitido por Sectigo (ya sea certificado de suscriptor o certificado de CA) se encuentra en la URL codificada dentro del campo CRLDP del propio certificado.

El perfil de Sectigo CRL es según la tabla siguiente:

Versión	[Versión 1]	
Nombre del emisor	DN del emisor, por ejemplo: CountryName = [nombre del país del certificado raíz], OrganizationName = [Organización de certificado raíz], CommonName = [Nombre común del certificado raíz] [Codificación PrintableString] O [Codificación UTF8String]	
Esta actualización	[Fecha de emisión]	
Próxima actualización	Certificados de entidad final: [<= Fecha de emisión + 10 días] Certificados de sub CA: [<= Fecha de emisión + 12 meses]	
Certificados revocados	Entradas de CRL	
	Número de serie del certificado	[Número de serie del certificado]
	Fecha y hora de revocación	[Fecha y hora de la revocación]

7.2.1. Número (s) de versión

Sectigo emite CRL de la versión 2.

7.2.2. Extensiones de entrada de CRL y CRL

Extensión	**Valor**
Número de CRL	Nunca se repite un número entero que aumenta monótonamente
Identificador de clave de autoridad	Igual que el identificador de la clave de autoridad que figura en el Certificado.
Fecha de invalidez	Fecha en formato UTC
Código de razón	Razón opcional para la revocación

7.3. Perfil OCSP

Sectigo publica información sobre el estado de los certificados mediante el Protocolo de estado de certificados en línea (OCSP). Los respondedores OCSP de Sectigo son capaces de proporcionar un estado 'bueno' o 'revocado' para todos los certificados emitidos bajo los términos de este CP. Los respondedores de OCSP darán una respuesta "desconocida" para los certificados caducados.

Sectigo opera un servicio OCSP en http://ocsp.sectigo.com. La información de revocación está disponible de inmediato a través de los servicios de OCSP. El respondedor OCSP y las respuestas están disponibles 24x7.

7.3.1. Número (s) de versión

El respondedor OCSP de Sectigo cumple con RFC 5019 y RFC 6960.

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Las prácticas especificadas en esta CP han sido diseñadas para cumplir o superar los requisitos de los estándares de la industria en desarrollo y generalmente aceptados, incluidos los estándares ETSI para proveedores de servicios de confianza y otros estándares de la industria relacionados con el funcionamiento de las CA.

Un auditor externo independiente evalua el cumplimiento de Sectigo con eIDAS y ETSI realizando una auditoría periódica.

8.1. Frecuencia o circunstancias de la evaluación

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

8.2. Identidad / calificaciones del auditor

Un CAB certificado o acreditado deberá realizar las auditorías ETSI / eIDAS.

En cualquier caso, un CAB significa un (grupo de) personas físicas o jurídicas 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 (ver 8.1);
- 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;
- Estar acreditado de acuerdo con ETSI EN 319 403, o acreditado para realizar tales auditorías bajo un esquema nacional equivalente, o acreditado por un organismo de acreditación nacional de acuerdo con ISO 17065;
- Obligado por la ley, la regulación gubernamental o el código de ética profesional

8.3. Relación del auditor con la entidad evaluada

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

8.4. Temas cubiertos por la auditoria

Los temas cubiertos por la auditoría incluyen, entre otros, los siguientes:

- Divulgación de prácticas comerciales,
    - el TSP divulga sus prácticas comerciales, y
    - el TSP presta sus servicios de acuerdo con su CPS
- Gestión del ciclo de vida de las claves,
    - el TSP mantiene controles efectivos para brindar una seguridad razonable de que la integridad de las claves y los certificados que administra está establecida y protegida a lo largo de sus ciclos de vida.
- Gestión del ciclo de vida del certificado, lo que significa que
    - El TSP mantiene controles efectivos para proporcionar una seguridad razonable de que la información del Suscriptor se autenticó adecuadamente para actividades de registro específicas, y
    - El TSP mantiene controles efectivos para proporcionar una seguridad razonable de que las solicitudes de certificados de CA subordinadas son precisas, autenticadas y aprobadas.
- Controles del TSP, lo que significa que
    - el TSP mantiene controles efectivos para proporcionar una seguridad razonable de que
        - El acceso lógico y físico a los sistemas y datos de CA está restringido a personas autorizadas,
        - Se mantiene la continuidad de las operaciones de gestión de claves y certificados, y
        - El desarrollo, el mantenimiento y las operaciones de los sistemas de CA están debidamente autorizados y realizados para mantener la integridad de los sistemas de CA.

8.5. Acciones tomadas como resultado de una deficiencia

El CAB acreditado informaría o documentaría la deficiencia y notificaría a Sectigo de los hallazgos. Dependiendo de la naturaleza y el alcance de la deficiencia, Sectigo desarrollaría un plan para corregir la deficiencia, lo que podría implicar cambiar sus políticas o prácticas, o ambas. Luego, Sectigo pondría en funcionamiento sus políticas o prácticas enmendadas y exigiría a los auditores que verifiquen que la deficiencia ya no está presente. Sectigo decidiría entonces si emprendería alguna acción correctiva con respecto a los certificados ya emitidos.

8.6. Comunicación de resultados

La auditoría requiere que Sectigo ponga el Informe de auditoría a disposición del público. No se requiere que Sectigo ponga a disposición del público ningún hallazgo de auditoría general que no afecte la opinión general de auditoría.

8.7. Auto auditorías

Sectigo realiza auto-auditorías y auditorías de las Autoridades de Registro de acuerdo con los diferentes estándares y las mejores prácticas y directrices de la industria.

9. OTROS ASUNTOS LEGALES Y COMERCIALES

9.1. Tarifa

Sectigo cobra tarifas de suscriptor por algunos de los servicios de certificación que ofrece. Sectigo se reserva el derecho de efectuar cambios en dichas tarifas. Se informará a los socios de Sectigo sobre las modificaciones de precios según se detalla en sus respectivos acuerdos.

9.1.1. Tarifas de emisión o renovación de certificados

Sectigo tiene derecho a cobrar a los Suscriptores por la emisión, administración y renovación de certificados. En la mayoría de las circunstancias, las tarifas de certificado aplicables se delinearán en el Acuerdo de Suscriptor entre Sectigo y el Suscriptor.

9.1.2. Tarifas de acceso al certificado

Sectigo no cobra una tarifa como condición para que un certificado esté disponible en un repositorio o para que los certificados estén disponibles para los terceros de confianza, pero puede cobrar una tarifa razonable por el acceso a sus bases de datos de certificados.

9.1.3. Tarifas de acceso a la información de estado o revocación

Sectigo no cobra tarifas por la revocación de un certificado o para que un tercero de confianza verifique el estado de validez de un certificado emitido por Sectigo utilizando CRL.

9.2. Responsabilidad financiera

9.2.1. Cobertura del seguro

Sectigo mantiene un seguro profesional de errores y omisiones.

9.3. Confidencialidad de la información comercial

Sectigo observa las normas aplicables sobre la protección de los datos personales que la ley o la política de privacidad de Sectigo (consulte la sección 9.4.1 de este CP) consideran confidenciales.

9.3.1. Alcance de la información confidencial

Sectigo mantiene la confidencialidad de los siguientes tipos de información y mantiene controles razonables para evitar la exposición de dichos registros a personal no confiable.

- Acuerdos de suscriptor.
- Registros y documentación de la solicitud de certificado presentados en apoyo de las solicitudes de certificado, ya sean exitosas o rechazadas.
- Registros de transacciones y registros de auditoría financiera.
- Registros e informes de seguimiento de auditoría externa o interna, excepto los informes de auditoría de eIDAS / ETSI que pueden publicarse a discreción de Sectigo.
- Claves privadas
- Planes de contingencia y planes de recuperación ante desastres.

- Rastreos y registros internos sobre las operaciones de la infraestructura de Sectigo, la gestión de certificados y los servicios y datos de inscripción.

9.3.2. Información que no está dentro del alcance de la información confidencial

Los suscriptores reconocen que los datos de revocación de todos los certificados emitidos por Sectigo son información pública y se publican cada 24 horas. Los datos de la solicitud del suscriptor marcados como "Públicos" en el Acuerdo del Suscriptor correspondiente, o enviados como parte de una solicitud de certificado para ser publicados dentro de un certificado emitido, no se consideran información confidencial.

9.3.3. Responsabilidad de proteger la información confidencial

Todo el personal en puestos de confianza maneja toda la información confidencial con estricta confidencialidad.

El personal de Sectigo, especialmente el de la RA / LRA, debe cumplir con los requisitos de las respectivas leyes sobre protección de información confidencial.

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

Sectigo ha implementado salvaguardas y protecciones de privacidad adecuadas, y sigue su Política de privacidad publicada, que cumple con este CP y la ley aplicable.

9.4.2. Información tratada como confidencial

Consulte la Política de privacidad. Además, la información personal obtenida de un solicitante durante el proceso de solicitud o verificación de identidad se considera información privada si la información no está incluida en el certificado y si la información no es información pública.

9.4.3. Información no considerada confidencial

Además de la información que no se considera privada en la Política de privacidad, la información que se hace pública en un certificado, CRL u OCSP no se considera privada.

9.4.4. Responsabilidad de proteger la información confidencial

Se espera que los participantes de Sectigo manejen la información privada con cuidado y de acuerdo con las leyes de privacidad locales en la jurisdicción relevante.

9.4.5. Aviso y consentimiento para usar información confidencial

Sectigo proporciona avisos a los solicitantes y suscriptores sobre el uso de información privada por parte de Sectigo a través de su Política de privacidad. Sectigo también proporciona avisos a los solicitantes y suscriptores sobre el uso de información privada por parte de Sectigo en el momento en que se recopila dicha información. Sectigo obtendrá el consentimiento de un solicitante o suscriptor para usar información privada según lo requieran las leyes o regulaciones aplicables.

9.4.6. Divulgación de conformidad con un proceso judicial o administrativo

La divulgación de información por parte de Sectigo de conformidad con un proceso judicial o administrativo se establece en la Política de privacidad. Sectigo se reserva el derecho de divulgar información si Sectigo cree razonablemente que la divulgación es requerida por ley o reglamento, o que la divulgación es necesaria en respuesta a un proceso judicial, administrativo u otro proceso legal.

9.5. Derechos de propiedad intelectual

Sectigo, o sus subsidiarias, afiliadas, otorgantes de licencias o asociados, poseen todos los derechos de propiedad intelectual sobre los servicios de Sectigo, incluidas las bases de datos, los sitios web, los certificados de Sectigo y cualquier otra publicación originada en Sectigo, incluido este CP.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la CA

Sectigo hace ciertas declaraciones con respecto a los servicios de certificados realizados de conformidad con este CP, como se describe a continuación. Sectigo se reserva el derecho de modificar dichas representaciones según lo considere oportuno o lo requiera la ley.

Salvo que se indique expresamente en este CP o en un acuerdo separado con el suscriptor, en la medida especificada en las secciones relevantes del CP, Sectigo representa a:

- Cumplir con este CP y sus políticas y procedimientos internos o publicados.
- Cumpla con las leyes y regulaciones aplicables.
- Proporcionar servicios de infraestructura y certificación, que incluyen, entre otros, el establecimiento y funcionamiento del Repositorio 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.
- Proporcione un aviso inmediato en caso de que se comprometa su (s) clave (s) privada (s).
- Proporcionar y validar los procedimientos de solicitud para los distintos tipos de certificados que puede poner a disposición.
- Emitir certificados de acuerdo con este CP y cumplir con sus obligaciones aquí presentadas.
- Al recibir una solicitud de una RA que opera dentro de la red Sectigo, actúe con prontitud para emitir un certificado de acuerdo con este CP.
- Al recibir una solicitud de revocación de un RA que opera dentro de la red Sectigo, actúe con prontitud para revocar un certificado Sectigo de acuerdo con este CP.
- Publicar los certificados aceptados de acuerdo con este CP.
- Revocar certificados de acuerdo con este CP.

- Prever la expiración y renovación de certificados de acuerdo con este CP.

Como la red de Sectigo incluye RA que operan bajo las prácticas y procedimientos de Sectigo, Sectigo garantiza la integridad de cualquier certificado emitido bajo su propia raíz dentro de los límites de las pólizas de seguro de Sectigo y de acuerdo con este CP.

El suscriptor reconoce que Sectigo no tiene más obligaciones en virtud de este CP.

9.6.2. Representaciones y garantías de la RA

Las RA de Sectigo operan bajo las políticas y prácticas detalladas en este CP y también el acuerdo asociado. La RA está obligada por contrato a:

- Recibir solicitudes de certificados Sectigo de acuerdo con este CP.
- Realice todas las acciones de verificación prescritas por los procedimientos de validación de Sectigo y este CP.
- Recibir, verificar y transmitir a Sectigo todas las solicitudes de revocación de un certificado de Sectigo de acuerdo con los procedimientos de revocación de Sectigo y este CP.
- Actúe de acuerdo con las leyes y regulaciones pertinentes.

9.6.3. Declaraciones y garantías de los suscriptores

Los suscriptores declaran y garantizan que cuando se envían a Sectigo y usan un dominio y un nombre distinguido (y toda otra información de solicitud de certificado) no interfieren ni infringen ningún derecho de terceros en ninguna jurisdicción con respecto a sus marcas comerciales, marcas de servicio, marcas comerciales nombres, nombres de empresas o cualquier otro derecho de propiedad intelectual, y que no pretenden utilizar el dominio y los nombres distinguidos para ningún fin ilícito, que incluye, entre otros, la interferencia ilícita con el contrato o una ventaja comercial prospectiva, la competencia desleal, dañar la reputación de otro, y confundir o inducir a error a una persona, ya sea natural o incorporada.

Al aceptar un certificado, el suscriptor declara a Sectigo y a las partes que confían que en el momento de la aceptación y hasta nuevo aviso:

- proporcionar información precisa y completa en todo momento a Sectigo en la solicitud de certificado y cuando se solicite en relación con la emisión de certificados;
- instale y use cada certificado 1) solo en los dominios que el suscriptor posea o controle y 2) solo en los servidores accesibles en el nombre de dominio que figura en el certificado si el certificado es un QWAC;
- utilizar los certificados únicamente para los fines enumerados en este CP;
- revisar y verificar la exactitud de los datos en cada certificado antes de instalar y usar el certificado, e informar inmediatamente a Sectigo si algún dato listado en un certificado cambia o deja de ser exacto;
- ser responsable, a expensas del suscriptor, de 1) todos los ordenadores, equipos de telecomunicaciones, software, acceso a Internet y redes de comunicaciones (si las

hubiera) requeridas para usar los certificados, 2) la conducta del suscriptor y el mantenimiento, operación, desarrollo y mantenimiento de su sitio web y contenido;
- informar de inmediato a Sectigo si el suscriptor se da cuenta de cualquier uso indebido de los certificados y ayudar a Sectigo a prevenir, curar y rectificar cualquier uso indebido;
- tomar todas las medidas razonables para asegurar el control, mantener la confidencialidad y proteger adecuadamente en todo momento la Clave Privada que corresponde a la Clave Pública que se incluirá en un certificado;
- Deje de usar de inmediato un certificado y la clave privada relacionada y solicite la revocación del certificado si 1) cualquier información en el certificado es o se vuelve incorrecta o inexacta, o 2) hay un uso indebido o comprometido real o sospechado de la clave privada asociada con el certificado;
- cesar todo uso del certificado y su clave privada al vencimiento o revocación del certificado;
- Cumplir con todas las regulaciones, políticas y procedimientos de sus redes mientras usa certificados,
- obtener y mantener en vigor cualquier consentimiento, autorización, permiso o licencia que pueda requerirse para el uso legal de los certificados por parte del suscriptor; y
- Cumplir con todas las leyes, reglas, regulaciones y pautas aplicables al usar un certificado.
- El suscriptor retiene el control de la clave privada, utiliza un sistema confiable y toma las precauciones razonables para evitar su pérdida, divulgación, modificación o uso no autorizado.
- El suscriptor es un suscriptor de usuario final y no una CA, y no utilizará la clave privada correspondiente a ninguna clave pública enumerada en el certificado con el fin de firmar ningún certificado (o cualquier otro formato de clave pública certificada) o CRL, como CA o de otro modo, a menos que se acuerde expresamente por escrito entre el suscriptor y Sectigo.

En todos los casos y para todos los tipos de certificados de Sectigo, el suscriptor tiene la obligación continua de monitorear la precisión de la información enviada y notificar a Sectigo de dichos cambios.

9.6.4. Declaraciones y garantías de las partes confiables

Una parte que confía en un certificado de Sectigo acepta y reconoce que para poder confiar razonablemente en un certificado de Sectigo, dicha parte debe:

- Minimizar el riesgo de depender de una firma electrónica o sello creado por un certificado inválido, revocado, vencido o rechazado; el tercero de confianza debe haber hecho un esfuerzo razonable para adquirir conocimientos suficientes sobre el uso de certificados y PKI.
- No usar un certificado, ni depender de un certificado, como equipo de control en circunstancias peligrosas o circunstancias que requieran un desempeño a prueba de fallos, como la operación de instalaciones nucleares, sistemas de comunicación o

navegación de aeronaves, sistemas de control de tráfico aéreo, sistemas de control de armas o similares. podría provocar directamente la muerte, lesiones personales o daños graves al medio ambiente, cada uno de los cuales es un uso no autorizado de un certificado y para el cual un certificado no está diseñado ni destinado.

- Estudie las limitaciones en el uso de certificados y conozca a través del contrato de Confianza el valor máximo de las transacciones que se pueden realizar utilizando un certificado Sectigo.
- Lea y acepte los términos del acuerdo de Sectigo CP y la parte que confía.
- Verifique un certificado de Sectigo consultando la CRL relevante y las CRL de la CA intermedia y la CA raíz o verificando la respuesta OCSP utilizando el respondedor Sectigo OCSP.
- Confíe en un certificado solo si es válido y no ha sido revocado o vencido.
- Confíe en un certificado, solo en la medida que sea razonable en las circunstancias enumeradas en esta sección y otras secciones relevantes de este CP.

9.7. Renuncias de garantías

9.7.1. Aptitud para un propósito particular

Sectigo renuncia a todas las garantías y obligaciones de cualquier tipo, incluida cualquier garantía de idoneidad para un propósito en particular, y cualquier garantía de la precisión de la información no verificada proporcionada, salvo lo contenido en este documento y que no pueda excluirse por ley.

9.7.2. Otras garantías

Salvo que se haya indicado lo contrario en relación con los Certificados Cualificados emitidos de conformidad con los requisitos del Reglamento Europeo 910/2014, Sectigo no garantiza:

- La precisión, autenticidad, integridad o idoneidad de cualquier información no verificada contenida en certificados o compilada, publicada o difundida de otra manera por Sectigo o en su nombre, excepto que se indique en la descripción del producto correspondiente a continuación en este CP y en la póliza de seguro de Sectigo.
- Además, no incurrirá en responsabilidad por las representaciones de la información contenida en un certificado, salvo que se indique en la descripción del producto correspondiente en este CP.
- No garantiza la calidad, las funciones o el rendimiento de ningún dispositivo de software o hardware.
- Aunque Sectigo es responsable de la revocación de un certificado, no puede ser considerado responsable si no puede ejecutarlo por razones ajenas a su control.
- La validez, integridad o disponibilidad de directorios de certificados emitidos por un tercero (incluido un agente) a menos que Sectigo lo indique específicamente.

Sectigo asume que el software de usuario que se afirma cumple con X.509v3 y otros estándares aplicables hace cumplir los requisitos establecidos en este CP. Sectigo no puede garantizar que

dicho software de usuario respaldará y hará cumplir los controles requeridos por Sectigo, mientras que el usuario debe buscar el asesoramiento adecuado.

9.8. Limitaciones de responsabilidad

Los certificados de Sectigo pueden incluir una breve declaración que describe las limitaciones de responsabilidad, las limitaciones en el valor de las transacciones a realizar, el período de validación y el propósito previsto del certificado y las renuncias de garantía que pueden aplicarse. Los suscriptores deben aceptar los Términos y condiciones de Sectigo, o un Acuerdo de suscriptor, antes de registrarse para obtener un certificado. Para comunicar información, Sectigo puede utilizar:

- Un atributo de unidad organizativa.
- Un calificador de recursos estándar de Sectigo para una política de certificados.
- Extensiones registradas de propietarios u otros proveedores.

9.8.1. Limitaciones de daños y pérdidas

En ningún caso (excepto por fraude o mala conducta intencional) la responsabilidad total de Sectigo hacia todas las partes, incluidos, entre otros, un suscriptor, un solicitante, un destinatario o un tercero de confianza por todas las firmas digitales y transacciones relacionadas con dicho certificado, excederá el valor acumulativo por dicho certificado como se indica en la sección detallada del plan de seguro Sectigo **Error! Reference source not found.** de este CP.

9.8.2. Exclusión de ciertos elementos de daños.

En ningún caso (excepto por fraude o mala conducta intencional) Sectigo será responsable de:

- Cualquier daño indirecto, incidental, consecuente o especial.
- Cualquier lucro cesante.
- Cualquier pérdida de datos.
- Cualquier otro daño indirecto, consecuente o punitivo que surja de o en conexión con el uso, entrega, licencia, desempeño o incumplimiento de certificados o firmas o sellos electrónicos.
- Cualquier otra transacción o servicio ofrecido en el marco de este CP.
- Cualquier otro daño, excepto los debidos a la confianza en la información que figura en un certificado, en la información verificada en un certificado.
- Cualquier responsabilidad incurrida en este caso o en cualquier otro caso si la falla en esta información verificada se debe a fraude o mala conducta intencional del solicitante. Cualquier responsabilidad que surja del uso de un certificado que no haya sido emitido o usado de conformidad con este CP.
- Cualquier responsabilidad que se derive del uso de un certificado que no sea válido.
- Cualquier responsabilidad que surja del uso de un certificado que exceda las limitaciones de uso y valor y transacciones indicadas en él o en el CP.
- Cualquier responsabilidad que surja de la seguridad, usabilidad, integridad de los productos, incluido el hardware y el software que utiliza un suscriptor.

- Cualquier responsabilidad que surja del compromiso de la clave privada de un suscriptor.

Sectigo no limita ni excluye la responsabilidad por muerte o lesiones personales.

9.9. Indemnizaciones

9.9.1. Indemnización por suscriptor

Al aceptar un certificado, el suscriptor acepta indemnizar y eximir a Sectigo, así como a sus agentes y contratistas de cualquier acto u omisión que resulte en responsabilidad, cualquier pérdida o daño, y cualquier demanda y gasto de cualquier tipo, incluidos los razonables. honorarios de abogados, en los que puedan incurrir Sectigo y las partes antes mencionadas, que sean causados por el uso o publicación de un certificado, y que surjan de:

- Cualquier dato falso o tergiversado proporcionado por el suscriptor o agente (s).
- Cualquier falla del suscriptor para revelar un hecho material, si la tergiversación u omisión se realizó por negligencia o con la intención de engañar a la CA, Sectigo o cualquier persona que reciba o confíe en el certificado.
- No proteger los datos confidenciales del suscriptor, incluida su clave privada, o no tomar las precauciones razonables necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de los datos confidenciales del suscriptor.
- Romper las leyes aplicables en su país o territorio, incluidas las relacionadas con la protección de la propiedad intelectual, virus, acceso a sistemas informáticos, etc.

Para los certificados emitidos a solicitud de un agente del suscriptor, tanto el agente como el suscriptor indemnizarán conjunta y solidariamente a Sectigo, sus agentes y contratistas.

Aunque Sectigo proporcionará toda la asistencia razonable, el suscriptor defenderá, indemnizará y eximirá de responsabilidad a Sectigo por cualquier pérdida o daño resultante de dicha interferencia o infracción y será responsable de defender todas las acciones en nombre de Sectigo.

9.10. Duración y Terminación

9.10.1. Término

El término de este CP, incluidas las enmiendas y los anexos, comienza con la publicación en el Repositorio y permanece en vigor hasta que sea reemplazado por un nuevo CP aprobado por la Autoridad de Políticas de Sectigo.

9.10.2. Terminación

Este CP, incluidas todas las enmiendas y adiciones, permanecerá en vigor hasta que sea reemplazado por una versión más reciente.

9.10.3. Efecto de terminación y supervivencia

Los siguientes derechos, responsabilidades y obligaciones sobreviven a la terminación de este CP para los certificados emitidos bajo este CP:

- Todas las tarifas impagas incurridas bajo la sección 9.1 de este CP;
- Todas las responsabilidades y obligaciones relacionadas con la información confidencial, incluidas las establecidas en la sección 9.3 de este CP;
- Todas las responsabilidades y obligaciones para proteger la información privada, incluidas las establecidas en la sección 9.4.4 de este CP;
- Todas las representaciones y garantías, incluidas las establecidas en la sección 9.6 de este CP;
- Todas las garantías denegadas en la sección 9.7 de este CP para certificados emitidos durante la vigencia de este CP;
- Todas las limitaciones de responsabilidad previstas en la sección 9.8 de este CP; y
- Todas las indemnizaciones previstas en el apartado 9.9 de este CP.

La terminación de este CP no afectará ningún Acuerdo de Suscriptor ejecutado durante la vigencia de este CP. Tras la terminación de este CP, todos los participantes de PKI están sujetos a los términos de este CP para los certificados emitidos durante la vigencia de este CP y por el resto de los períodos de validez de dichos certificados.

9.11. Avisos individuales y comunicaciones con los participantes

Sectigo acepta avisos relacionados con este CP mediante mensajes firmados digitalmente o en papel. Al recibir un acuse de recibo válido y firmado digitalmente de Sectigo, el remitente del aviso considerará que su comunicación es efectiva. El remitente debe recibir dicho acuse de recibo dentro de los cinco (5) días o, de lo contrario, se debe enviar un aviso por escrito en papel a través de un servicio de mensajería que confirme la entrega o por correo certificado o registrado, con franqueo prepagado, con acuse de recibo solicitado, con la siguiente dirección:

Autoridad de políticas de Sectigo
3.er piso, 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, Reino Unido
Correo electrónico: legalnotices@sectigo.com

9.12. Enmiendas

Una vez que la Autoridad de Políticas de Sectigo acepte dichos cambios que considere que tienen un impacto significativo en los usuarios de este CP, Sectigo, con siete (7) días de notificación de los próximos cambios, comunicará la versión actualizada de este CP a los usuarios correspondientes a través del correo registrado, correo electrónico, publicación en el repositorio de Sectigo o de otro modo. Una numeración de versión incremental adecuada utilizada para identificar una nueva versión indicará una versión actualizada de este CP.

Las revisiones que no se indican como “significativas” son aquellas que la Autoridad de Política de Sectigo considera que tienen un impacto mínimo o nulo en los suscriptores y los terceros de

confianza que utilizan certificados y CRL emitidos por Sectigo. Dichas revisiones pueden realizarse sin previo aviso a los usuarios del CP y sin cambiar el número de versión de este CP.

Existen controles para garantizar razonablemente que el Sectigo CP no se modifique ni se publique sin la autorización previa de la Autoridad de Políticas de Sectigo.

9.12.1. Procedimiento de modificación

La Autoridad de Política de Sectigo puede realizar una enmienda a este CP. La Autoridad de Políticas de Sectigo aprobará las enmiendas a este CP y Sectigo publicará las enmiendas en el Repositorio. Las enmiendas pueden ser una actualización, revisión o modificación de este documento de CP, y se pueden detallar en este CP o en un documento separado. Además, las enmiendas reemplazan cualquier disposición designada o en conflicto de la versión enmendada del CP.

9.12.2. Mecanismo y período de notificación

Sectigo notifica una enmienda al CP al publicarlo en el Repositorio. Las enmiendas entran en vigencia en la fecha provista en el documento, cuando una enmienda se escribe en un documento separado, o en la fecha provista en esta CP, cuando está escrita en este documento.

Sectigo no garantiza ni establece un período de notificación y comentario.

9.12.3. Circunstancias bajo las cuales se debe cambiar el OID

La Autoridad de Política de Sectigo tiene la autoridad exclusiva para determinar si una enmienda al CP requiere un cambio de OID.

9.13. Disposiciones de resolución de disputas

Antes de recurrir a cualquier mecanismo de resolución de disputas, incluida la adjudicación o cualquier tipo de resolución alternativa de disputas (incluido, sin excepción, un mini juicio, arbitraje, asesoramiento de expertos vinculantes, supervisión de la cooperación y asesoramiento de expertos normales), todas las partes acuerdan notificar a Sectigo de la disputa con una vista para buscar la resolución de disputas.

9.14. Ley aplicable, interpretación y jurisdicción

9.14.1. Ley que rige

Este CP se rige e interpreta de acuerdo con el reglamento eIDAS. Esta elección de la ley se realiza para garantizar una interpretación uniforme de este CP, independientemente del lugar de residencia o lugar de uso de los certificados de Sectigo u otros productos y servicios. La regulación eIDAS se aplica en todas las relaciones comerciales o contractuales de Sectigo en las que este CP pueda aplicarse o citarse implícita o explícitamente en relación con los productos y servicios de Sectigo donde Sectigo actúa como proveedor, proveedor, beneficiario receptor o de otro modo.

9.14.2. Interpretación

Este CP se interpretará de manera coherente dentro de los límites de las costumbres comerciales, la razonabilidad comercial en las circunstancias y el uso previsto de un producto o servicio. Al interpretar esta CP, las partes también deberán tener en cuenta el alcance internacional y la aplicación de los servicios y productos de Sectigo y su red internacional de RA, así como el principio de buena fe tal como se aplica en las transacciones comerciales.

Los títulos, subtítulos y otros títulos en este CP están destinados únicamente a fines de conveniencia y referencia y no se utilizarán para interpretar, interpretar o hacer cumplir cualquiera de las disposiciones de este CP.

Los apéndices y definiciones de este CP son, a todos los efectos, parte integrante y vinculante del CP.

9.14.3. Jurisdicción

Cada parte, incluidos los socios, suscriptores y las partes que confían de Sectigo, acuerda irrevocablemente que los tribunales de Barcelona en España tienen jurisdicción exclusiva para conocer y decidir cualquier demanda, acción o procedimiento, y para resolver cualquier disputa que pueda surgir de o en conexión con este CP o la prestación de los servicios de Sectigo.

9.15. Cumplimiento de la ley aplicable

Este CP 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. En la prestación de sus servicios PKI, Sectigo cumple en todos los aspectos materiales con las normas internacionales de alto nivel, incluidas las relativas a los certificados cualificados de conformidad con el Reglamento europeo 910/2014 y la ley pertinente sobre firmas electrónicas y todas las demás leyes y reglamentos pertinentes.

9.16. Otras disposiciones

9.16.1. Acuerdo completo

Este CP y todos los documentos a los que se hace referencia en este documento constituyen el acuerdo completo entre las partes, reemplazando todos los demás acuerdos que puedan existir con respecto al tema en cuestión. Los títulos de las secciones son solo para referencia y conveniencia y no forman parte de la interpretación de este acuerdo.

9.16.2. Asignación

Este CP será vinculante para los sucesores, albaceas, herederos, representantes, administradores y cesionarios, ya sea expreso, implícito o aparente de las partes. Los derechos y obligaciones detallados en este CP son asignables por las partes, por aplicación de la ley (incluso como resultado de una fusión o una transferencia de una participación mayoritaria en valores con derecho a voto) o de otro modo, siempre que dicha asignación se lleve a cabo de conformidad con los artículos de este CP sobre terminación o cese de operaciones, y siempre

que dicha cesión no produzca una novación de otras deudas u obligaciones que la parte cedente tenga con otras partes en el momento de dicha cesión.

9.16.3. Divisibilidad

Si alguna disposición de este CP o la aplicación del mismo, por cualquier motivo y en cualquier medida se considera inválida o inaplicable, el resto de este CP (y la aplicación de la disposición inválida o inaplicable a otras personas o circunstancias) se interpretará de tal manera que afecte la intención original de las partes.

Todas y cada una de las disposiciones de este CP que establecen una limitación de responsabilidad, exención de responsabilidad o limitación de cualquier garantía u otras obligaciones, o la exclusión de daños, está destinada a ser separable e independiente de cualquier otra disposición y debe hacerse cumplir como tal.

9.16.4. Ejecución (honorarios de abogados y renuncia de derechos)

Este CP se hará cumplir en su totalidad, mientras que el incumplimiento por parte de cualquier persona de hacer cumplir cualquier disposición de este CP no se considerará una renuncia a la aplicación futura de esa o cualquier otra disposición.

9.16.5. Fuerza mayor

Ni Sectigo ni ningún tercero independiente RA que opere bajo una Autoridad de Certificación de Sectigo, ni ningún revendedor, co-comercializador, ni ningún subcontratista, distribuidor, agente, proveedor, empleado o director de cualquiera de los anteriores incurrirá en incumplimiento o responsabilidad por cualquier pérdida, costo, gasto, responsabilidad, daño, reclamo o monto de liquidación que surja de o esté relacionado con demoras en el desempeño o por incumplimiento de los términos de Sectigo CP, cualquier Acuerdo de suscripción o cualquier Acuerdo de parte que confía debido a cualquier causa fuera de su control razonable, que incluye causas fortuitas o del enemigo público, disturbios e insurrecciones, guerras, accidentes, incendios, huelgas y otras dificultades laborales (esté o no Sectigo en condiciones de ceder a tales demandas) , embargos, acción judicial, falla o incumplimiento de cualquier autoridad de certificación superior, falta o incapacidad para obtener permisos o aprobaciones de exportación, materiales de mano de obra necesarios, energía, servicios públicos, componentes o maquinaria, actos de autoridades civiles o militares.

9.16.6. Conflicto de reglas

Cuando este CP entra en conflicto con otras reglas, pautas o contratos, este CP prevalecerá y obligará al suscriptor y a otras partes, excepto en lo que respecta a otros contratos:

- Antes del primer lanzamiento público de la presente versión de este CP.
- Reemplazando expresamente este CP por lo que dicho contrato regirá en cuanto a las partes del mismo, y en la medida permitida por la ley.

9.17. Otras provisiones

9.17.1. Responsabilidad del suscriptor con los terceros de confianza

Sin limitar otras obligaciones del suscriptor establecidas en este CP, los suscriptores son responsables de cualquier tergiversación que hagan en los certificados a terceros que se basen razonablemente en las representaciones contenidas en los mismos y hayan verificado una o más firmas electrónicas o sellos con el certificado.

9.17.2. Deber de supervisar a los agentes

El suscriptor controlará y será responsable de los datos que un agente suministre a Sectigo. El suscriptor debe notificar de inmediato al emisor de cualquier tergiversación u omisión realizada por un agente. El deber de este artículo es continuo.

9.17.3. Propiedad

Los certificados son propiedad de Sectigo. Sectigo da permiso para reproducir y distribuir certificados de forma no exclusiva y libre de regalías, siempre que se reproduzcan y distribuyan en su totalidad. Sectigo se reserva el derecho a revocar el certificado en cualquier momento. Las claves públicas y privadas son propiedad de los suscriptores que legítimamente las emiten y las poseen. Todas las acciones de la clave privada de Sectigo siguen siendo propiedad de Sectigo.

9.17.4. Interferencia con la implementación de Sectigo

Los suscriptores, los terceros de confianza y cualquier otra parte no interferirán ni aplicarán ingeniería inversa en la implementación técnica de los servicios de PKI de Sectigo, incluido el proceso de generación de claves, el sitio web público y los repositorios de Sectigo, excepto según lo permita explícitamente este CP o previa aprobación por escrito. de Sectigo. El incumplimiento de esto como suscriptor resultará en la revocación del certificado del suscriptor sin previo aviso al suscriptor y el suscriptor deberá pagar cualquier cargo pagadero pero que aún no se haya pagado bajo el acuerdo. El incumplimiento de esto como tercero de confianza resultará en la terminación del acuerdo con el tercero de confianza, la eliminación del permiso para usar o acceder al repositorio de Sectigo y cualquier certificado o Servicio proporcionado por Sectigo.

9.17.5. Elección del método criptográfico

Las partes son las únicas responsables de haber ejercido un juicio independiente y empleado la capacitación adecuada para elegir el software de seguridad, el hardware y los algoritmos de cifrado / firma digital, incluidos sus respectivos parámetros, procedimientos y técnicas, así como PKI como una solución a sus requisitos de seguridad.

9.17.6. Limitaciones de las asociaciones de Sectigo

Los socios de la red Sectigo no emprenderán acciones que puedan poner en peligro, poner en duda o reducir la confianza asociada a los productos y servicios de Sectigo. Los socios de Sectigo se abstendrán específicamente de buscar asociaciones con otros TSP. El incumplimiento de esto resultará en la terminación del acuerdo con el tercero de confianza, la eliminación del permiso

para usar o acceder al repositorio de Sectigo y cualquier certificado o Servicio Digital proporcionado por Sectigo.

9.17.7. Obligaciones del suscriptor

Salvo que se indique lo contrario en este CP, los suscriptores serán los únicos responsables:

- Minimizar el riesgo interno de compromiso de la clave privada asegurando que se proporcione internamente el conocimiento y la capacitación adecuados sobre PKI.
- Generar su propio par de claves pública / privada para usar en asociación con la solicitud de certificado enviada a Sectigo o Sectigo RA.
- Asegúrese de que la clave pública enviada a Sectigo o Sectigo RA corresponda con la clave privada utilizada.
- Asegúrese de que la clave pública enviada a Sectigo o Sectigo RA sea la correcta.
- Brindar información correcta y veraz en sus comunicaciones con Sectigo o un Sectigo RA.
- Avise a Sectigo o Sectigo RA si en cualquier etapa mientras el certificado es válido, cualquier información enviada originalmente ha cambiado desde que fue enviada a Sectigo.
- Genere un nuevo par de claves seguras para usar junto con un certificado que solicite a Sectigo o Sectigo RA.
- Lea, comprenda y acepte todos los términos y condiciones de este Sectigo CP y las políticas asociadas publicadas en el Repositorio de Sectigo en https://www.sectigo.com/legal/
- Abstenerse de manipular un certificado Sectigo.
- Utilice los certificados de Sectigo para fines legales y autorizados de acuerdo con los usos y prácticas sugeridos en este CP.
- Deje de usar un certificado de Sectigo si cualquier información que contenga se vuelve obsoleta o no válida.
- Deje de usar un certificado de Sectigo si dicho certificado está vencido y elimínelo de cualquier aplicación y / o dispositivo en el que se haya instalado.
- Abstenerse de utilizar la clave privada del suscriptor correspondiente a la clave pública en un certificado emitido por Sectigo para emitir certificados de entidad final o CA subordinadas.
- Hacer todos los esfuerzos razonables para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de la clave privada correspondiente a la clave pública publicada en un certificado de Sectigo.
- Solicitar la revocación de un certificado en caso de que ocurra algo que afecte materialmente la integridad de un certificado de Sectigo.
- Por actos y omisiones de socios y agentes, estos utilizan para generar, retener, custodiar o destruir sus claves privadas.

Apéndice A: ChangeLog

Versión	Cambiar Descripción	Fecha
1.0	Crear un nuevo CP para certificados cualificados eIDAS	1 de agosto de 2020
1.0.1	Actualizar CP en consecuencia con CPS	20 de agosto de 2020
1.0.2	Actualice la sección 3.2 y elimine algunas otras secciones	17 de septiembre de 2020
1.0.3	Se corrigieron algunos errores tipográficos y se actualizaron algunas URL.	19 de octubre de 2020
1.0.4	Aclaración de las secciones 1.1 y 3.2.5	20 de octubre de 2020
1.0.5	Se corrigieron algunos errores tipográficos en 1.6.1, se eliminó una oración poco clara en 3.1.5 y se agregaron los dominios de transición para la verificación CAA en 4.2.4 como en la CPS.	22 de octubre de 2020