Sectigo eIDAS Declaración de prácticas de Certificación

Sectigo (Europe) SL
Versión 1.0.14
Efectivo: 23 de Diciembre de 2022
Rambla Catalunya, 86 3 1,
08008 Barcelona, España
www.sectigo.com

Aviso de copyright

Copyright 2022 Sectigo. Reservados todos los derechos.

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

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

SECTIGO

Contenido

1. INTRODUCCIÓN 10

1.1. Visión general 10

1.2. Nombre e identificación del documento 10

1.3. Participantes de PKI 11
1.3.1. Autoridades de certificación 11
1.3.2. Autoridades de registro 12
1.3.3. Suscriptores (entidades finales) 13
1.3.4. Terceros de confianza 13
1.3.5. Otros participantes 14

1.4. Uso del certificado 14
1.4.1. Usos apropiados de los certificados 15
1.4.2. Usos prohibidos de certificados 16

1.5. Administración de políticas 16
1.5.1. Organización que administra el documento 16
1.5.2. Persona de contacto 16
1.5.3. Persona que determina la idoneidad de la DPC 17
1.5.4. Procedimientos de aprobación de la DPC 17

1.6. Definiciones y acrónimos 17
1.6.1. Siglas 17
1.6.2. Definiciones 20

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPOSITARIO 28

2.1. Repositorios 28

2.2. Publicación de información de certificación 28

2.3. Frecuencia de publicación 28

2.4. Controles de acceso en repositorios 29

2.5. Exactitud de la información 29

3. IDENTIFICACIÓN Y AUTENTICACIÓN 30

3.1. Nombres 30
3.1.1. Tipos de nombres 30
3.1.2. Necesidad de que los nombres sean significativos 30
3.1.3. Anonimato o seudonimato de los suscriptores. 30
3.1.4. Reglas para interpretar varias formas de nombres 30
3.1.5. Unicidad de nombres 30
3.1.6. Reconocimiento, autenticación y rol de las marcas registradas 31

3.2. Validación de identidad inicial 31

3.2.1. Autenticación de la identidad de una persona física 31
3.2.2. Autenticación de la identidad de una persona jurídica 33
3.2.3. QWAC 34
3.2.4. PSD2 40
3.2.5. Método para demostrar la posesión de la clave privada 40
3.2.6. Validación de autoridad 41
3.2.7. Criterios de interoperación 41
3.2.8. Validación de la solicitud 41

3.3. Identificación y autenticación para solicitudes de renovación de claves 42
3.3.1. Identificación y autenticación para el cambio de clave 42
3.3.2. Identificación y autenticación para la nueva generación de claves después de la revocación 42

3.4. Identificación y autenticación para solicitud de revocación 42

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO 44

4.1. Solicitud de certificado 44
4.1.1. Quién puede enviar una solicitud de certificado 45
4.1.2. Proceso de inscripción y responsabilidades 45

4.2. Procesamiento de solicitud de certificado 46
4.2.1. Realización de funciones de identificación y autenticación 46
4.2.2. Aprobación o rechazo de solicitudes de certificado 47
4.2.3. Tiempo de procesamiento de las solicitudes de certificados 47
4.2.4. Autorización de la autoridad de certificación (solo para QWAC) 47

4.3. Emisión de certificados 48
4.3.1. Acciones de CA durante la emisión del certificado 48
4.3.2. Notificación al suscriptor por parte de la CA de la emisión del certificado 49
4.3.3. Negativa a emitir un certificado 50

4.4. Aceptación del certificado 50
4.4.1. Conducta que constituye la aceptación del certificado 50
4.4.2. Publicación del certificado por la CA 50
4.4.3. Notificación de la emisión del certificado por parte de la CA a otras entidades 50

4.5. Par de claves y uso de certificados 51
4.5.1. Uso de certificado y clave privada del suscriptor 51
4.5.2. Uso de certificado y clave pública de parte de confianza 51

4.6. Renovación de certificado 52
4.6.1. Circunstancia para la renovación del certificado 52
4.6.2. Quién puede solicitar la renovación 52
4.6.3. Procesamiento de solicitudes de renovación de certificados 52
4.6.4. Notificación de la emisión de un nuevo certificado al suscriptor 52
4.6.5. Conducta que constituye la aceptación de un certificado de renovación 52
4.6.6. Publicación del certificado de renovación por parte de la CA 53
4.6.7. Notificación de la emisión del certificado por parte de la CA a otras entidades 53

4.7. Cambio de clave de un certificado 53
4.7.1. Circunstancias para la renovación de claves del certificado 53

4.7.2. Quién puede solicitar el cambio de clave del certificado 53
4.7.3. Procesamiento de solicitudes de renovación de claves de certificados 53
4.7.4. Notificación de cambio de clave al suscriptor 53
4.7.5. Conducta que constituye la aceptación de un certificado con clave nueva 54
4.7.6. Publicación del certificado con nueva clave por parte de la CA 54
4.7.7. Notificación de la emisión del certificado por parte de la CA a otras entidades 54

4.8. Modificación de un certificado 54

4.9. Revocación y suspensión de certificados 54
4.9.1. Circunstancias para la revocación 54
4.9.2. Quién puede solicitar la revocación 56
4.9.3. Procedimiento de solicitud de revocación 56
4.9.4. Tiempo dentro del cual Sectigo procesará la solicitud de revocación 56
4.9.5. Requisito de verificación de revocación para los terceros de confianza 57
4.9.6. Frecuencia de emisión de CRL 57
4.9.7. Latencia máxima para las CRL 57
4.9.8. Disponibilidad de verificación de estado / revocación en línea 58
4.9.9. Requisitos de verificación de revocación en línea 58

4.10. Servicios de estado de certificados 59
4.10.1. Características operativas 59
4.10.2. Servicio disponible 59

4.11. Fin de suscripción 59

4.12. Depósito y recuperación de claves 59

5. CONTROLES OPERATIVOS, DE GESTIÓN Y DE INSTALACIONES 60

5.1. Controles físicos 60
5.1.1. Ubicación y construcción del sitio (CPD) 60
5.1.2. Acceso físico 60
5.1.3. Energía y aire acondicionado 60
5.1.4. Exposiciones al agua 60
5.1.5. Prevención y protección contra incendios 61
5.1.6. Almacén de datos 61
5.1.7. Depósito de basura 61
5.1.8. Copia de seguridad fuera del sitio 61

5.2. Controles de procedimiento 61
5.2.1. Roles de confianza 61
5.2.2. Número de personas necesarias por tarea 63
5.2.3. Identificación y autenticación para cada rol 63

5.3. Controles de personal 63
5.3.1. Requisitos de calificaciones, experiencia y autorización 63
5.3.2. Procedimientos de verificación de antecedentes 64
5.3.3. Requisitos de formación 64
5.3.4. Frecuencia y requisitos de formación 64
5.3.5. Sanciones por acciones no autorizadas 64
5.3.6. Requisitos del contratista independiente 65
5.3.7. Documentación suministrada al personal 65

5.4. Procedimientos de registro de auditoría 65
5.4.1. Tipos de eventos registrados 65
5.4.2. Registro de frecuencia de procesamiento 66
5.4.3. Período de retención del registro de auditoría 66
5.4.4. Protección del registro de auditoría 67
5.4.5. Procedimientos de copia de seguridad del registro de auditoría 67
5.4.6. Sistema de recopilación de auditorías (interno frente a externo) 67
5.4.7. Evaluaciones de vulnerabilidad 67

5.5. Archivo de registros 68
5.5.1. Tipos de registros archivados 68
5.5.2. Periodo de conservación del archivo 68
5.5.3. Protección de archivo 68
5.5.4. Procedimientos de respaldo de archivos 68
5.5.5. Requisitos para el sellado de tiempo de los registros 69
5.5.6. Sistema de recopilación de archivos (interno o externo) 69
5.5.7. Procedimientos para obtener y verificar información de archivo 69

5.6. Cambio de clave 69

5.7. Compromiso y recuperación ante desastres 70
5.7.1. Procedimientos de gestión de incidentes 70
5.7.2. Los recursos informáticos, el software y / o los datos están dañados 70
5.7.3. Procedimientos de compromiso de clave privada de la CA 71
5.7.4. Procedimientos de compromiso de algoritmos 71
5.7.5. Capacidades de continuidad empresarial después de un desastre 71

5.8. Finalización del TSP 71

6. CONTROLES DE SEGURIDAD TÉCNICA 73

6.1. Generación e instalación del par de claves 73
6.1.1. Generación del par de claves 73
6.1.2. Entrega de la clave privada al suscriptor 75
6.1.3. Entrega de la clave pública al emisor del certificado 75
6.1.4. Entrega de la clave pública de CA a los terceros de confianza 76
6.1.5. Tamaños de clave 76
6.1.6. Generación de parámetros de la clave pública 76
6.1.7. Propósitos de uso de claves (según el campo de uso de claves X.509v3) 76

6.2. Protección de la clave privada y controles del módulo criptográfico 77
6.2.1. Estándares y controles de módulos criptográficos 77
6.2.2. Transferencia de la clave privada hacia o desde un módulo criptográfico 78
6.2.3. Almacenamiento de la clave privada en módulo criptográfico 78
6.2.4. Método de activación de la clave privada 78
6.2.5. Método para desactivar la clave privada 78
6.2.6. Método de destrucción de la clave privada 78
6.2.7. Calificación del módulo criptográfico 78

6.3. Otros aspectos de la gestión de los pares de claves 79
6.3.1. Archivo de la clave pública 79
6.3.2. Períodos operativos del certificado y períodos de uso del par de claves 79

6.4. Datos de activación 79

6.4.1. Generación e instalación de los datos de activación 79
6.4.2. Protección de los datos de activación 80

6.5. Controles de seguridad informática 80
6.5.1. Requisitos técnicos específicos de seguridad informática 80

6.6. Controles técnicos del ciclo de vida 81
6.6.1. Controles de desarrollo del sistema 81
6.6.2. Controles de gestión de seguridad 81

6.7. Controles de seguridad de la red 82

6.8. Sello de tiempo 82

7. PERFILES DE CERTIFICADOS, CRL Y OCSP 83

7.1. Perfil del certificado 83
7.1.1. Número (s) de versión 84
7.1.2. Extensiones del certificado 84
7.1.3. Identificadores de objetos de algoritmo 86
7.1.4. Formas de nombres 86
7.1.5. Restricciones de nombres 87
7.1.6. Identificador de objeto de política de certificado 87
7.1.7. Sintaxis y semántica de las políticas 88

7.2. Perfil de CRL 88
7.2.1. Número (s) de versión 89
7.2.2. Extensiones de entrada de CRL 89

7.3. Perfil OCSP 90
7.3.1. Número (s) de versión 91

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES 92

8.1. Frecuencia o circunstancias de la evaluación 92

8.2. Identidad / Cualificaciones del evaluador 92

8.3. Relación del evaluador con la entidad evaluada 92

8.4. Temas cubiertos por la evaluación 92

8.5. Acciones a realizar como resultado de una deficiencia 93

8.6. Comunicación de resultados 93

8.7. Auto-auditorías 94

9. OTROS ASUNTOS LEGALES Y COMERCIALES 95

9.1. Tarifa 95
9.1.1. Tarifas de emisión o renovación de certificados 95

9.1.2. Tarifas de acceso al certificado 95
9.1.3. Tarifas de acceso a la información de estado o revocación 95
9.1.4. Politica de reembolso 95
9.1.5. Política de reemisión 95

9.2. Responsabilidad financiera 96
9.2.1. Cobertura del seguro 96
9.2.2. Cobertura de seguro o garantía para entidades finales 96

9.3. Confidencialidad de la información comercial 96
9.3.1. Alcance de la información confidencial 96
9.3.2. Información que no está dentro del alcance de la información confidencial 97
9.3.3. Responsabilidad de proteger la información confidencial 97
9.3.4. Publicación de datos de revocación de certificados 97

9.4. Privacidad de la información personal 97
9.4.1. Plan de privacidad 97
9.4.2. Información tratada como confidencial 97
9.4.3. Información no considerada confidencial 97
9.4.4. Responsabilidad de proteger la información confidencial 97
9.4.5. Aviso y consentimiento para usar información confidencial 98
9.4.6. Divulgación de conformidad con un proceso judicial o administrativo 98
9.4.7. Otras circunstancias de divulgación de información 98

9.5. Derechos de propiedad intelectual 98

9.6. Representaciones y garantías 98
9.6.1. Representaciones y garantías de la CA 98
9.6.2. Representaciones y garantías de la RA 99
9.6.3. Declaraciones y garantías de los suscriptores 99
9.6.4. Declaraciones y garantías de los terceros de confianza 101

9.7. Renuncias de garantías 101
9.7.1. Aptitud para un propósito particular 101
9.7.2. Otras garantías 101

9.8. Limitaciones de responsabilidad 102
9.8.1. Limitaciones de daños y pérdidas 102
9.8.2. Exclusión de ciertos elementos de daños. 102

9.9. Indemnizaciones 103
9.9.1. Indemnización por Sectigo 103
9.9.2. Indemnización por suscriptor 103
9.9.3. Indemnización por parte de las partes que confían 104

9.10. Duración y Terminación 104
9.10.1. Término 104
9.10.2. Terminación 104
9.10.3. Efecto de terminación y supervivencia 104

9.11. Avisos individuales y comunicaciones con los participantes 105

9.12. Enmiendas 105
9.12.1. Procedimiento de modificación 105
9.12.2. Mecanismo y período de notificación 105

9.12.3. Circunstancias bajo las cuales se debe cambiar el OID 106

9.13. Disposiciones de resolución de disputas 106

9.14. Ley aplicable, interpretación y jurisdicción 106
9.14.1. Ley que rige 106
9.14.2. Interpretación 106
9.14.3. Jurisdicción 106

9.15. Cumplimiento de la ley aplicable 107

9.16. Otras disposiciones 107
9.16.1. Acuerdo completo 107
9.16.2. Asignación 107
9.16.3. Divisibilidad 107
9.16.4. Ejecución (honorarios de abogados y renuncia de derechos) 107
9.16.5. Fuerza mayor 107
9.16.6. Conflicto de reglas 108

9.17. Otras provisiones 108
9.17.1. Responsabilidad del suscriptor ante los terceros de confianza 108
9.17.2. Deber de vigilar a los agentes 108
9.17.3. Propiedad 108
9.17.4. Interferencia con la implementación de Sectigo 109
9.17.5. Elección del método criptográfico 109
9.17.6. Limitaciones de las asociaciones de Sectigo 109
9.17.7. Obligaciones del suscriptor 109

ANEXO A: JERARQUÍA Y PERFILES DE CA CUALIFICADOS 111

Certificado raíz 111

Certificado de CA emisora 111

Certificado raíz 111

Certificado de CA emisora 112

Certificado raíz 112

Certificado de CA emisora 113

Certificado END ENTITY 113

ANEXO B: TIPOS DE CERTIFICADOS CUALIFICADOS SECTIGO 114

ANEXO C: CHANGELOG 116

ANEXO D: BIBLIOGRAFÍA 119

1. INTRODUCCIÓN

Sectigo es un proveedor de servicios de confianza (TSP) que emite certificados digitales confiables a entidades, incluidas empresas públicas y privadas, y personas físicas de acuerdo con esta Declaración de prácticas de certificación (DPC).

Este documento define las diferentes prácticas para la PKI cualificada de Sectigo, que rige la emisión y gestión de certificados cualificados.

En su rol de CA (Autoridad de Certificación), Sectigo realiza funciones asociadas con operaciones de clave pública que incluyen recibir solicitudes, emitir, revocar y renovar certificados digitales y el mantenimiento, emisión y publicación de Listas de Revocación de Certificados (CRLs) para usuarios dentro de la Infraestructura de clave pública (PKI) de Sectigo.

1.1. Visión general

Sectigo sigue el Reglamento de la UE 910/2014 de 23 de julio de 2014 sobre identificación electrónica y servicios de confianza para transacciones electrónicas en el Mercado Único Europeo, derogando la directiva 1999/93 / EC del 13 de diciembre de 1999, comúnmente denominada eIDAS.

Para la emisión de certificados de servidor seguro cualificados específicos para sitios web, también denominados QWAC, Sectigo también cumple con la última versión de los Requisitos de referencia (BR) y las Directrices EV (EVG) del CAB Forum. En caso de cualquier inconsistencia entre esta DPC y los otros documentos especificados en este párrafo, esos documentos tienen prioridad sobre esta DPC.

Sectigo puede extender, 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 por Sectigo.

Esta DPC es solo uno de un conjunto de documentos relevantes para la prestación de servicios de certificación por Sectigo y que la lista de documentos contenidos en esta cláusula son otros documentos que esta DPC mencionará de vez en cuando, aunque esta no es una lista exhaustiva.

Esta DPC, los acuerdos relacionados y las políticas de certificados a las que se hace referencia en este documento están disponibles en *www.sectigo.com/legal*.

1.2. Nombre e identificación del documento

Este documento es la Declaración de prácticas de certificación (DPC) de Sectigo para certificados cualificados. Describe los principios y prácticas legales, comerciales y técnicos que Sectigo emplea en la prestación de servicios de certificación que incluyen, entre otros, la aprobación, emisión, uso y gestión de certificados digitales y el mantenimiento de una

infraestructura de clave pública basada en certificados X.509 (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. Esta DPC también es un medio de notificación de roles y responsabilidades para las partes involucradas en prácticas basadas en certificados dentro de la PKI cualificada de Sectigo.

Esta DPC de Sectigo es una declaración pública de las prácticas de Sectigo y las condiciones de emisión, revocación y renovación de un certificado emitido bajo la propia jerarquía de Sectigo.

Esta DPC está estructurada siguiendo el estándar RFC 3647 del Internet Engineering Task Force (IETF).

Para identificar individualmente cada tipo de certificado cualificado emitido por Sectigo de acuerdo con esta Declaración de Prácticas de Certificación, se asigna un identificador de objeto (OID) a cada tipo.

Se pueden encontrar en el documento de perfiles disponible en *www.sectigo.com/eidascps*.

También de acuerdo con la definición de ETSI EN 319 412-5, Sectigo incluye algunos de los identificadores QcStatements.

1.3. Participantes de PKI

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

1.3.1. Autoridades de certificación

En su función de CA, Sectigo proporciona servicios de certificados dentro de la PKI cualificada de Sectigo. Consulte el anexo A para ver la PKI cualificada por Sectigo. Sectigo hará:

- Ajustar sus operaciones a esta DPC (u otra divulgación de prácticas comerciales de CA), ya que la misma puede ser modificada 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 DPC,
- Al recibir una solicitud válida para revocar el certificado de una persona autorizada para solicitar la revocación utilizando los métodos de revocación detallados en esta DPC, revocar un certificado emitido para su uso dentro de la PKI cualificada de Sectigo,
- Publicar CRL de forma regular, de acuerdo con la Política de Certificados aplicable y con las disposiciones descritas en esta DPC,
- Distribuir los certificados emitidos de acuerdo con los métodos detallados en esta DPC,

- Actualizar las CRL de manera oportuna como se detalla en esta DPC,
- Notificar a los suscriptores por correo electrónico de la inminente expiración de su certificado emitido por Sectigo (por un período divulgado en esta DPC).

1.3.2. Autoridades de registro

Sectigo ha establecido la infraestructura segura necesaria para administrar completamente el ciclo de vida de los certificados cualificados dentro de su PKI. A través de una red de RA, Sectigo también pone sus servicios de autoridad de certificación a disposición de sus suscriptores. Sectigo RA:

- Aceptar, evaluar, aprobar o rechazar el registro de solicitudes de certificado.
- Verificar la exactitud y autenticidad de la información proporcionada por el suscriptor en el momento de la solicitud como se especifica en esta DPC, siguiendo la regulación eIDAS y los estándares ETSI para certificados y sellos cualificados y en documentación adicional como los BR y EVG para QWAC.
- Utilizar un documento oficial, notariado o indicado de otro modo para evaluar una solicitud de suscriptor.
- Verificar la exactitud y autenticidad de la información proporcionada por el suscriptor en el momento de la reemisión o renovación como se especifica en esta DPC, las normas BR y EVG y ETSI y el reglamento eIDAS.

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.

Para certificados QWAC, Sectigo puede extender el uso de RA para su revendedor de alojamiento web. Tras la aprobación para unirse al programa respectivo, se le puede permitir actuar como RA en nombre de Sectigo. Las RA deben cumplir con esta DPC, los BR y EVG y el reglamento eIDAS.

Las RA solo pueden realizar sus tareas de validación a partir de sistemas pre aprobados que se identifican ante 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 CA intermedias desde las cuales emite certificados cualificados.

1.3.2.1. Autoridad de registro interno

Sectigo opera su propia RA interna que permite a los clientes minoristas, así como a todos los clientes de Socios revendedores, junto con algunos de los revendedores de servidores web de Sectigo, administrar el ciclo de vida de sus certificados, incluida la aplicación, emisión, renovación y revocación. La RA de Sectigo se adhiere a la DPC de Sectigo.

Para la emisión de QWAC, esta RA también está equipada con sistemas automatizados que validan el control de dominio. Para esa minoría de QWAC para los que la validación del control de dominio no es posible por medios completamente automatizados, el personal especialmente capacitado y examinado que Sectigo emplea en su RA tiene la capacidad de provocar la emisión de certificados, pero solo cuando están autenticados en los sistemas de emisión que utilizan autenticación de dos factores de Sectigo.

La RA interna de Sectigo, junto con su personal y sistemas, se encuentran dentro del alcance de los requisitos de auditoría de Sectigo.

1.3.2.2. Autoridad de registro externa

Sectigo puede autorizar a algunos revendedores o clientes empresariales para actuar como RA externos. Como tales, se les puede conceder la funcionalidad de RA que puede incluir la validación de parte o toda la información de identidad del sujeto. La RA externa está obligada a realizar la validación de acuerdo con esta DPC, las BR y las normas EVG del CAB Forum y las normas ETSI y el reglamento eIDAS antes de emitir un certificado y reconoce haber validado suficientemente la identidad del solicitante. Este reconocimiento puede ser a través de un proceso en línea, o mediante los parámetros de API de que se ha realizado una validación suficiente antes de que Sectigo emita un certificado o mediante cualquier otro método que demuestre la identidad del solicitante / suscriptor.

Las RA externas no validan el control de dominio para los QWAC. La RA interna de Sectigo como se describe en esta DPC siempre realiza este elemento de la validación de los QWAC.

1.3.3. Suscriptores (entidades finales)

Los suscriptores de los servicios de Sectigo son personas físicas o jurídicas que utilizan PKI en relación con las transacciones y comunicaciones respaldadas por 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.

Consulte el Anexo B para obtener información adicional sobre los diferentes certificados cualificados emitidos por Sectigo.

1.3.4. Terceros de confianza

Los terceros de confianza utilizan los servicios PKI en relación con varios certificados cualificados de Sectigo para los fines previstos y pueden confiar razonablemente en dichos certificados y / o firmas digitales verificables con referencia a una clave pública incluida en un certificado de suscriptor.

Para verificar la validez de un certificado cualificado que reciben, estos terceros de confianza deben consultar la CRL o la respuesta del Protocolo de Estado de Certificados en Línea (OCSP) antes de confiar en la información incluida en un certificado para asegurarse de que Sectigo no

haya revocado el certificado. La ubicación de la CRL se detalla en el certificado. Las respuestas OCSP se envían a través del respondedor OCSP.

Además, todos los certificados cualificados se compararán con la TSL correspondiente.

1.3.5. Otros participantes

Sectigo tiene varias categorías de socios, que ayudan en la prestación de servicios de certificación, como socios revendedores y revendedores de alojamiento web. Todos estos socios ayudan en los servicios de ventas pero no están relacionados con el ciclo de vida de los certificados.

1.3.5.1. Socios revendedores

Sectigo opera una red de socios revendedores que permite a los socios autorizados integrar certificados cualificados de Sectigo en sus propias carteras de productos. Los socios revendedores son responsables de derivar a los clientes de certificados a Sectigo, quien mantiene un control total sobre el proceso del ciclo de vida del certificado, incluida la aplicación, emisión, renovación y revocación. Debido a la naturaleza del programa de revendedor, el socio revendedor debe autorizar un pedido de cliente pendiente realizado a través de su cuenta de socio revendedor antes de que Sectigo instigue la validación de dichos pedidos de certificados. Todos los socios revendedores deben proporcionar una prueba del estado de la organización y deben firmar un acuerdo de socio revendedor de Sectigo antes de que se les proporcionen las instalaciones de socio revendedor.

El programa de revendedores de alojamiento web es un tipo específico de socio revendedor que permite a las organizaciones que ofrecen servicios de alojamiento gestionar el ciclo de vida del certificado en nombre de sus clientes alojados. Dichos revendedores de servidores web pueden solicitar certificados cualificados, generalmente QWAC, en nombre de sus clientes alojados.

Todos los revendedores de alojamiento web deben proporcionar prueba del estado de la organización y deben firmar un contrato de revendedor de alojamiento web de Sectigo antes de que se les proporcionen las autorizaciones como revendedor.

1.4. Uso del certificado

Un certificado digital son datos formateados que vinculan criptográficamente a un suscriptor identificado con una clave pública. Un Certificado digital permite a una persona física o jurídica que participa en una transacción electrónica demostrar su identidad a otros participantes en dicha transacción.

Actualmente, Sectigo ofrece una cartera de certificados digitales, con la consideración de productos cualificados y relacionados que se pueden utilizar para abordar las necesidades de los usuarios para comunicaciones personales y comerciales seguras, que incluyen, entre otros,

correo electrónico seguro, protección de transacciones en línea e identificación de personas, ya sean legales o físicas, o dispositivos en una red o dentro de una comunidad.

Sectigo puede actualizar o ampliar su lista de productos, incluidos los tipos de certificados que emite, según lo considere oportuno.

1.4.1. Usos apropiados de los certificados

Como se detalla en esta DPC, Sectigo ofrece una gama de distintos tipos de certificados cualificados. Los diferentes tipos de certificados cualificados tienen diferentes usos previstos y diferentes políticas. Los precios y las tarifas de suscripción de estos certificados están disponibles en los sitios web oficiales de Sectigo correspondientes. La garantía máxima asociada a cada certificado se detalla en la sección 9.2.3 de esta DPC.

Dado que el uso sugerido para un certificado cualificado difiere según la aplicación, se insta a los suscriptores a estudiar adecuadamente sus requisitos para su aplicación específica antes de solicitar un certificado específico. Los certificados revocados se referencian adecuadamente en las CRL y se publican en los directorios de Sectigo.

1.4.1.1. QWAC

Por lo general, los QWAC, también conocidos como certificados SSL o TLS, facilitan el intercambio de claves de cifrado para permitir la comunicación cifrada de información a través de Internet entre el usuario de un navegador de Internet y un sitio web.

El reglamento eIDAS define los certificados de sitios web cualificados de la UE que se utilizan para respaldar la autenticación de sitios web. Estos certificados se pueden emitir a personas físicas y jurídicas. Cuando este tipo de certificado se emite a una persona jurídica, se incorporan todos los requisitos de los certificados EV más las disposiciones adicionales que se especifican en eIDAS. También se puede emitir a personas jurídicas de acuerdo con la directiva de servicios de pago de la UE 2015/2366, denominada PSD2.

Los QWAC pueden contener varios FQDN o direcciones IP en el campo subjectAlternativeName.

1.4.1.2. Certificados cualificados para firmas / sellos electrónicos

Estos certificados se emiten de acuerdo con el reglamento eIDAS ofreciendo el nivel de cualificado según el reglamento. Estos certificados se pueden emitir a una persona física para que se utilicen para firmar o se pueden emitir a personas jurídicas para que se utilicen para sellar. Dependiendo del dispositivo utilizado, QSCD o no, para estas acciones se puede considerar si la firma o el sello es cualificado.

Como se indica en 1.4.1.1, existe un tipo específico de certificados cualificados para la autenticación de sitios web, comúnmente llamado QWAC.

Los sellos también se pueden emitir a entidades de acuerdo con la directiva de servicios de pago de la UE 2015/2366.

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.

1.5. Administración de políticas

La información que se encuentra en esta sección incluye la información de contacto de la organización responsable de redactar, registrar, mantener, actualizar y aprobar esta DPC.

1.5.1. Organización que administra el documento

La Autoridad de Políticas de Sectigo mantiene esta DPC, los acuerdos relacionados y las políticas de certificación a las que se hace referencia en este documento.

La Autoridad de Políticas (PA):

- Establece y mantiene esta DPC.
- 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 esta DPC se realicen de acuerdo con los requisitos, representaciones y garantías de la CP.

1.5.2. Persona de contacto

Se puede contactar con la autoridad de políticas en la siguiente dirección:

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

Para informar de un abuso, uso fraudulento o malintencionado de certificados cualificados emitidos por Sectigo, se puede envíar un correo electrónico a *qcabuse@sectigo.com*

Sectigo también opera diferentes alternativas para solicitar una revocación automatizada. Todos estos métodos se pueden encontrar en: *https://sectigo.com/support/revocation*

Recomendamos el uso de nuestro portal de revocación automatizado, o ACME revokeCert para una respuesta más rápida a los problemas que requieren revocación.

1.5.3. Persona que determina la idoneidad de la DPC

La Autoridad de Políticas de Sectigo es responsable de determinar la idoneidad de las políticas de certificados en esta DPC. La Autoridad de Políticas de Sectigo también es responsable de determinar la idoneidad de los cambios propuestos a esta DPC antes de la publicación de una edición enmendada.

1.5.4. Procedimientos de aprobación de la DPC

Esta DPC y cualquier cambio, enmienda o adición posterior, serán aprobados por la Autoridad de Políticas de Sectigo como se especifica en el documento de Procedimientos y Membresía de la Autoridad de Políticas de Sectigo (PA).

1.6. Definiciones y acrónimos

La lista de definiciones y acrónimos que se encuentran en esta sección son para uso dentro de la DPC de Sectigo.

1.6.1. Siglas

Los acrónimos y abreviaturas utilizados a lo largo de esta DPC deberán representar las frases o palabras que se establecen a continuación:

Acrónimo	**Nombre completo**
ADN	Autorizacion de nombre de dominio
BR	Requisitos básicos
CA	autoridad de certificación
CAB	Organismo de evaluación de la conformidad
CA/B	Autoridad de certificación / navegador (foro)
CMS	Sistema de gestión de certificados
CP	Política de certificado
PA	Autoridad de políticas
DPC	Declaración de prácticas de certificación
CRL(s)	Lista(s) de revocación de certificados
CSR	Solicitud de firma de certificado
CT	Transparencia del certificado

DBA	Haciendo negocios como
DN	Nombre distinguido
DSA	Algoritmo de firma digital
ECDSA	Algoritmo de firma digital de curva elíptica
eIDAS	Servicios electrónicos de identificación, autenticación y confianza
ESI	Firmas e Infraestructuras Electrónicas
ETSI	Instituto Europeo de Normas y Telecomunicaciones
EV	Validación extendida
EVG	Directrices EV
FIPS PUB	Publicación de estándares federales de procesamiento de información
FQDN	nombre de dominio completo
FTP	Protocolo de transferencia de archivos
GDPR	Reglamento general de protección de datos
HSM	Módulo de seguridad de hardware
HTTP	Protocolo de Transferencia de Hipertexto
ICANN	Corporación de Internet para la Asignación de Nombres y Números
IEC	Comisión Electrotécnica Internacional
ISO	Organización Internacional de Normalización
ITU	Unión Internacional de Telecomunicaciones
ITU-T	Sector de Normalización de las Telecomunicaciones de la UIT
LDAP	Protocolo ligero de acceso a directorios
LRA	RA local
MDC	Certificado de dominio múltiple
NCA	Autoridad Nacional Competente
NIST	Instituto Nacional de Estándares y Tecnología

NTP	Protocolo de tiempo de red
OCSP	Protocolo de estado de certificado en línea
OID	Identificador de objeto
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
PSP	Proveedor de servicios de pago
QSCD	Dispositivo cualificado de creación de firma / sello
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
SB	Organismo supervisor
S/MIME	Extensiones de correo de Internet seguras / multipropósito
SSL	Capa de sockets seguros
TLS	Transport Layer Security
TSA	Autoridad de Sellado de Tiempo
TSL	Lista de servicios de confianza
TSP	Proveedor de servicios de confianza
UTC	Hora universal coordinada

URL	Localizador Uniforme de Recursos

1.6.2. Definiciones

Los términos en mayúscula utilizados a lo largo de esta DPC tendrán los significados que se establecen a continuación:

Término	**Definición**
Firma electrónica avanzada	Significa una firma electrónica que cumple los requisitos establecidos en el artículo 26 del reglamento eIDAS.
Sello electrónico avanzado	significa un sello electrónico, que cumple los requisitos establecidos en el artículo 36 del reglamento eIDAS
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 el suscriptor. Para los certificados emitidos para dispositivos, el solicitante es la persona física o jurídica que controla u opera el dispositivo mencionado en el certificado, incluso si el dispositivo está enviando la solicitud de certificado real.
Representante del solicitante	Significa una persona física 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.
Informe de auditoria	Significa un informe de un CAB que expresa la opinión del CAB sobre si los procesos y controles de un TSP cumplen con las disposiciones obligatorias de la regulación eIDAS y los estándares ETSI.
Nombre de dominio de autorización	Hace referencia al nombre de dominio utilizado para obtener la autorización para la emisión de certificados para un FQDN determinado.
Numero de autorización	Un identificador único de un proveedor de servicios de pago que actúa como suscriptor de los certificados PSD2. El número de autorización es utilizado y reconocido por la NCA.

Restricciones básicas	Significa una extensión que especifica si el sujeto del certificado puede actuar como una CA o solo como una entidad final.
Requisitos básicos (BR)	Hace referencia a los requisitos básicos de CA / Browser Forum para la emisión y gestión de certificados de confianza pública, publicados en *https://www.cabforum.org*.
Certificado	clave pública de un usuario, junto con alguna otra información, convertida en imposible de falsificar mediante el cifrado con la clave privada de la autoridad de certificación que la emitió
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 del certificado, 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; certificados de publicación; almacenar certificados; almacenar 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.
Gerente de certificado	Significa el software emitido por Sectigo y utilizado por los Suscriptores para descargar certificados.
Política de certificado	Significa una declaración del emisor que corresponde al uso prescrito de un certificado digital dentro de un contexto de emisión.
Sistemas de certificación	Hace referencia al sistema utilizado por Sectigo o un tercero delegado para proporcionar verificación de identidad, registro e inscripción, aprobación de certificados, emisión, estado de validez, soporte y otros servicios relacionados con la PKI.

Transparencia del certificado	Significa el protocolo descrito en RFC 6962 para registrar públicamente la existencia de certificados de seguridad de la capa de transporte (TLS) a medida que se emiten u observan.
autoridad de certificación	Autoridad en la que confían uno o más usuarios para crear y asignar certificados. Una CA puede ser: 1) un proveedor de servicios de confianza que crea y asigna certificados de clave pública; o 2) un servicio de generación de certificados técnicos que es utilizado por un proveedor de servicios de certificación que crea y asigna certificados de clave pública.
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 proporciona
Cuenta de depósito a la vista	una cuenta de depósito mantenida en un banco u otra institución financiera, cuyos fondos depositados son pagaderos a la vista. El propósito principal de las cuentas a la vista es facilitar los pagos sin efectivo mediante cheque, giro bancario, débito directo, transferencia electrónica de fondos, etc. El uso varía entre países, pero una cuenta de depósito a la vista se conoce comúnmente como: una cuenta corriente, un giro bancario, etc.
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 de DNS.
Nombre de dominio	Significa la etiqueta asignada a un nodo en el Sistema de nombres de dominio.
Registrante de nombre de dominio	Hace referencia a las personas físicas o jurídicas registradas con un Registrador de nombres de dominio que tienen derecho a controlar cómo se utiliza un Nombre de dominio, como la persona física o jurídica que aparece como el "Registrante" por WHOIS o el Registrador de nombres de dominio. y, a veces, se lo denomina el "propietario" de un nombre de dominio.

Registrador de nombres de dominio	Significa una persona física o jurídica 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;
Estándares ETSI	Significa, individual o colectivamente, los documentos elaborados por el Comité Técnico ESI de ETSI con requisitos aplicables a un Certificado.
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 en euros (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 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)	Directrices de CA/Browser Forum para la emisión y gestión de certificados de validación extendida publicados en *https://www.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.
Autoridad de registro de direcciones IP	La Autoridad de Números Asignados de Internet (IANA) o un Registro Regional de Internet (RIPE, APNIC, ARIN, AfriNIC, LACNIC).
Sistema emisor	Significa un sistema utilizado para firmar certificados o información sobre el estado de validez.
Persona legal	Significa una asociación, corporación, sociedad, propiedad, fideicomiso, entidad gubernamental u otra entidad con personalidad jurídica en el sistema legal de un país.
Autoridad Nacional Competente	Una autoridad nacional responsable de los servicios de pago. La NCA aprueba o rechaza las autorizaciones para los proveedores de servicios de pago en su país.
Identificador de objeto	Se refiere a los números de identificación únicos organizados jerárquicamente, que en particular permiten hacer referencia a las condiciones aplicables al servicio de confianza prestado.
Proveedor de servicios de pago	Una organización autorizada para proporcionar servicios de pago a los clientes.
Precertificado	Significa un certificado que se construye a partir del certificado que se emitirá agregando una extensión especial de veneno crítico con el propósito de enviarlo a un registro de CT de acuerdo con RFC 6962
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 solo con la clave privada correspondiente del titular.
Certificado cualificado	En el contexto del Reglamento (UE) 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) 910/2014 (eIDAS), significa un certificado para una firma electrónica emitido por un proveedor de servicios de confianza cualificado.
Certificado cualificado para sello electrónico	En el contexto del Reglamento (UE) 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 (QSCD)	En el contexto del Reglamento (UE) 910/2014 (eIDAS), significa 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 (QTSP)	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 (QWAC)	En el contexto del Reglamento (UE) 910/2014 (eIDAS), se entiende un certificado de identificación de 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.
Autoridad de Registro	Entidad que se encarga de la identificación y autenticación de los sujetos de los certificados principalmente. Un RA puede ayudar en el proceso de solicitud de certificado o en el proceso de revocación o en ambos.
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 que no sea el Representante solicitante.
Tercero de confianza	Significa una entidad que confia en la información contenida en el certificado.
Acuerdo del tercero de confianza	significa un acuerdo entre Sectigo y un tercero que confía que debe ser leído y aceptado por un tercero que confía antes de validar, confiar o usar un certificado y está disponible para referencia en el Repositorio.
Repositorio	Significa el repositorio de Sectigo, disponible en *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.
Autoridad de políticas de Sectigo	Significa la entidad encargada del mantenimiento y publicación de las declaraciones de políticas y prácticas.
Sistema de soporte de seguridad	Hace referencia a un sistema utilizado 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.

Sujeto	entidad identificada en un certificado como el titular de la clave privada asociada con la clave pública proporcionada en el certificado
Suscriptor	Persona jurídica o física vinculada por acuerdo con un proveedor de servicios de confianza a cualquier obligación del suscriptor.
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.
Organismo supervisor	Un organismo responsable de las tareas de supervisión en el estado miembro de la UE que lo designa, según se define en el artículo 17 de eIDAS.
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
Método de comunicación verificado	Método de comunicación definido y verificado de conformidad con la Sección 11.5 de la EVG
X.509	Significa el estándar ITU-T para certificados y su marco de autenticación correspondiente.

2. RESPONSABILIDADES DE PUBLICACIÓN Y DEPOSITARIO

Sectigo publica esta DPC, los términos y condiciones, el Acuerdo de terceros de confianza y copias de todos los Acuerdos de Suscriptor 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 esta DPC.

La información crítica publicada puede actualizarse de vez en cuando según lo prescrito en esta DPC. Dichas actualizaciones se indicarán mediante la numeración de versión adecuada y la fecha de publicación en cualquier versión nueva.

2.1. Repositorios

Sectigo publica un repositorio de avisos legales sobre sus servicios PKI, incluyendo esta DPC, acuerdos y avisos, referencias dentro de esta DPC, así como cualquier otra información que considere esencial para sus servicios. Se puede acceder al repositorio en *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:

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

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

Además del repositorio, Sectigo aloja páginas web de prueba para QWAC que permiten a los proveedores de software de aplicaciones de terceros probar su software que se conecta a los certificados raíz de Sectigo. Sectigo también incluye en el repositorio certificados de prueba para firmas y sellos.

2.3. Frecuencia de publicación

Las versiones actualizadas o modificadas de los Acuerdos de suscriptor y los Acuerdos de terceros de confianza generalmente se publican dentro de los siete días posteriores a la aprobación. Esta DPC se revisa y se publican versiones actualizadas o modificadas al menos una vez al año y de acuerdo con la sección 9.12 de esta DPC. Para conocer la frecuencia de emisión de CRL, consulte la sección 4.9.6 de esta DPC.

2.4. Controles de acceso en repositorios

Los documentos publicados en el Repositorio son y serán de información pública y el acceso es de libre acceso. Sectigo cuenta con medidas de control de acceso lógico y físico 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 esta DPC y la póliza de seguro de Sectigo.

3. IDENTIFICACIÓN Y AUTENTICACIÓN

Sectigo ofrece diferentes tipos de certificados cualificados. Antes de la emisión de un certificado cualificado, Sectigo validará una solicitud de acuerdo con esta DPC que puede involucrar la solicitud por parte de Sectigo al solicitante de la documentación oficial relevante que respalde la solicitud.

Sectigo lleva a cabo la gestión general de la certificación dentro de la PKI cualificada de Sectigo; ya sea directamente o a través de una RA aprobada por Sectigo.

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.

En el caso de los QWAC, en general, incluye entradas en la extensión subjectAlternateName (SAN) que están destinadas a los terceros de confianza, por ejemplo, los navegadores.

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.

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 ITU-T X.520.

3.1.5. Unicidad de nombres

Sectigo no reasigna un sujeto distinguishName (DN) que se ha utilizado en un certificado a otro sujeto.

Sectigo incluye en el campo del número de serie del sujeto los identificadores semánticos según ETSI EN 319 412-1 para certificados de personas físicas y el identificador de organización para personas jurídicas.

Sectigo asigna los números de serie de los certificados que aparecen en los certificados de Sectigo. Los números de serie asignados son únicos. Sectigo genera al menos números de serie de 64 bits. Estos números son el resultado de un CSPRNG. Sectigo tiene una verificación de

unicidad separada que verifica que los números de serie del certificado nunca se vuelvan a utilizar.

3.1.6. Reconocimiento, autenticación y rol de las marcas registradas

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 esta DPC, 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

Sectigo realiza la identificación y autenticación de los solicitantes utilizando cualquier medio legal de comunicación o investigación para validar la identidad de estas personas físicas o jurídicas. Los procedimientos, así como las descripciones de los campos, se describen a continuación para cada tipo de certificado emitido.

Sectigo no emite certificados por sí mismo salvo los necesarios para la correcta gestión de los servicios prestados.

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 digital, otros requisitos de la industria o según lo prescrito por la ley.

3.2.1. Autenticación de la identidad de una persona física

El propósito de estos Certificados Cualificados de la UE es identificar al suscriptor con un alto nivel de garantía, con el propósito de:

- Creación de Firmas Electrónicas Cualificadas que cumplan con los requisitos de cualificación definidos por el Reglamento eIDAS. Estos certificados utilizan un QSCD para la protección de la clave privada. Estos certificados cumplen con la “Política para certificados cualificados de la UE de ETSI emitidos a una persona física donde la clave privada y el certificado relacionado residen en un QSCD” (QCP-n-qscd).
- Creación de Firmas Electrónicas Avanzadas que cumplan con los requisitos de calificación definidos por el Reglamento eIDAS. Estos certificados no utilizan un QSCD para la protección de la clave privada. Estos certificados cumplen con la "Política para certificados cualificados de la UE emitidos a una persona física" de ETSI (QCP-n).

El contenido de estos certificados cumple los requisitos pertinentes de:

- ETSI EN 319 412-1: Perfiles de certificados; Parte 1: descripción general y estructuras de datos comunes
- ETSI EN 319 412-2: Perfiles de certificados; Parte 2: Perfil de certificado para certificados expedidos a personas físicas
- ETSI EN 319 412-5: Perfiles de certificados; Parte 5: qcStatements

3.2.1.1. Proceso de verificación de identidad

Los procedimientos de validación de identidad para estos certificados cumplen con los requisitos relevantes de ETSI EN 319 411-2.

Sectigo recomienda que los certificados QCP-n-qcsd y QCP-n se utilicen solo para firmas electrónicas.

Se comprobará la identidad de la persona física y, en su caso, cualquier atributo específico de la persona:

- por la presencia física de la persona física; o
- utilizando métodos que proporcionen una garantía equivalente en términos de fiabilidad a la presencia física y para los que Sectigo pueda demostrar la equivalencia. La prueba de equivalencia se puede realizar de acuerdo con el Reglamento eIDAS.

Se proporcionarán pruebas de:

- Nombre completo (incluido el apellido y los nombres de pila de conformidad con la ley aplicable y las prácticas de identificación nacional); y
- Fecha y lugar de nacimiento, referencia a un documento de identidad reconocido a nivel nacional u otros atributos que puedan utilizarse para, en la medida de lo posible, distinguir a la persona de otras con el mismo nombre.

La RA puede proporcionar pruebas en nombre del sujeto. Sin embargo, el sujeto sigue siendo responsable del contenido del certificado.

Si el suscriptor es una persona física que se identifica en asociación con una entidad organizativa, persona jurídica, se deberá proporcionar evidencia adicional de:

- Nombre completo y condición jurídica de la entidad organizativa asociada;
- Cualquier información de registro existente relevante (por ejemplo, registro de la empresa) de la entidad organizativa; y
- Evidencia de que el suscriptor está asociado con la entidad organizativa.

Los certificados que requieren un QSCD cumplen los requisitos establecidos en el Anexo II del Reglamento eIDAS.

Las obligaciones del suscriptor (o, respectivamente, las obligaciones del TSP que administra la clave en su nombre) requieren que la clave privada se mantenga (o, respectivamente, se use) bajo el control exclusivo del sujeto.

3.2.2. Autenticación de la identidad de una persona jurídica

El propósito de estos Certificados Cualificados de la UE es identificar al suscriptor con un alto nivel de garantía, con el propósito de:

- Creación de Sellos Electrónicos Cualificados que cumplan con los requisitos de cualificación definidos por el Reglamento eIDAS. Estos certificados utilizan un QSCD para la protección de la clave privada. Estos certificados cumplen con la "Política de certificado cualificado de la UE de ETSI emitido a una persona jurídica donde la clave privada y el certificado relacionado residen en un QSCD" (QCP-l-qscd).
- Creación de Sellos Electrónicos Avanzados que cumplan con los requisitos de calificación definidos por el Reglamento eIDAS. Estos certificados cumplen con la "Política para certificados cualificados de la UE emitidos a una persona jurídica" de ETSI (QCP-l).

El contenido de estos certificados cumple los requisitos pertinentes de:

- ETSI EN 319 412-1: Perfiles de certificados; Parte 1: descripción general y estructuras de datos comunes
- ETSI EN 319 412-3: Perfiles de certificados; Parte 3: Perfil de certificado para certificados emitidos a personas jurídicas
- ETSI EN 319 412-5: Perfiles de certificados; Parte 5: qcStatements
- ETSI TS 119 495: Perfiles de certificados cualificados y requisitos de la política de TSP según la Directiva de servicios de pago (UE) 2015/2366 para el tipo de certificados PSD2

3.2.2.1. Proceso de verificación de identidad

Los procedimientos de validación de identidad para estos certificados cumplen con los requisitos relevantes de ETSI EN 319 411-2.

Sectigo recomienda que los certificados QCP-l-qcsd y QCP-l se utilicen solo para sellos electrónicos.

Se comprobará la identidad de la persona jurídica y, en su caso, los atributos específicos de la persona:

- por la presencia física de un representante autorizado de la persona jurídica; o
- utilizando métodos que proporcionen una garantía equivalente en términos de fiabilidad a la presencia física y para los que Sectigo pueda demostrar la equivalencia. La prueba de equivalencia se puede realizar de acuerdo con el Reglamento eIDAS.

Se proporcionarán pruebas de:

- Nombre completo de la persona jurídica de acuerdo con las prácticas de identificación nacionales o de otro tipo aplicables; y

- En su caso, la asociación entre la persona jurídica y la otra entidad organizativa identificada en asociación con esta persona jurídica que aparecería en el atributo de organización del certificado, de conformidad con las prácticas de identificación nacionales u otras aplicables.

En el caso del representante autorizado de la persona jurídica, se aportará prueba de:

- Nombre completo (incluido el apellido y los nombres de pila de conformidad con la ley aplicable y las prácticas de identificación nacional); y
- Fecha y lugar de nacimiento, referencia a un documento de identidad reconocido a nivel nacional u otros atributos que puedan utilizarse para, en la medida de lo posible, distinguir a la persona de otras con el mismo nombre.

Los certificados que requieren un QSCD cumplen los requisitos establecidos en el Anexo II del Reglamento eIDAS.

Las obligaciones del suscriptor (o, respectivamente, las obligaciones del TSP que administra la clave en su nombre) requieren que la clave privada se mantenga (o, respectivamente, se use) bajo el control exclusivo del sujeto.

3.2.3. QWAC

Los certificados QWAC se pueden emitir a personas físicas o jurídicas.

El propósito de estos Certificados Cualificados de la UE es identificar al suscriptor con un alto nivel de garantía de un sitio web, cumpliendo con los requisitos de calificación definidos por el Reglamento eIDAS.

Estos certificados cumplen con la “Política para certificados cualificados de la UE emitidos a sitios web de personas físicas o jurídicas” de ETSI (QCP-w).

El contenido de estos Certificados cumple con los requisitos relevantes de:

- ETSI EN 319 412-1: Perfiles de certificados; Parte 1: descripción general y estructuras de datos comunes
- ETSI EN 319 412-4: Perfiles de certificados; Parte 4: perfil de certificado para certificados de sitios web
- ETSI EN 319 412-5: Perfiles de certificados; Parte 5: qcStatements

Los procedimientos de validación de identidad para estos certificados cumplen con los requisitos relevantes de ETSI EN 319 411-2 para la "Política para certificados cualificados de la UE emitidos a sitios web de personas físicas o jurídicas" (QCP-w) y las directrices de CA/B Forum.

3.2.3.1. Proceso de verificación de identidad

Sectigo garantiza que toda la información que se incluirá en el QWAC cumple con los requisitos y se verifica de acuerdo con las Directrices de CA/Browser Forum para la emisión y gestión de certificados de validación extendida (comúnmente denominados Directrices EV) en el caso de los QWAC emitidos a personas jurídicas y la ETSI EN 319 411-2.

Independientemente del proceso de identificación de la persona física o jurídica, Sectigo verificará el contenido de cada nombre de dominio o dirección IP incluidos en un Certificado de autenticación de sitio web cualificado.

3.2.3.1.1. Verificación de dominio

Para cada nombre de dominio que se incluirá en un QWAC, Sectigo verifica el control del solicitante sobre el nombre de dominio de acuerdo con los Requisitos básicos del CAB Forum, sección 3.2.2.4, utilizando uno de los siguientes métodos para cada FQDN:

1. Comunicarse directamente con el contacto del dominio utilizando una dirección postal, dirección de correo electrónico, FAX o SMS según la sección 3.2.2.4.2 de los BRs del CAB Forum;

    a. Comunicación directa con el registrador de dominios usando un Correo electrónico, fax, SMS o correo postal al contacto del dominio. Confirmar el control del solicitante sobre el FQDN enviando un valor aleatorio por correo electrónico, fax, SMS o correo postal a un destinatario identificado como un contacto de dominio y luego recibir una respuesta de confirmación utilizando el valor aleatorio. El valor aleatorio, que es único, es generado por Sectigo y sigue siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su generación;

2. Construir un email para contactar con el contacto del dominio según la sección 3.2.2.4.4 de los BRs (requisitos básicos) del CAB Forum

    Comunicarse directamente con el contacto del dominio confirmando el control del solicitante sobre el FQDN solicitado utilizando una dirección de correo electrónico construida mediante:

    a. enviar un correo electrónico a una o más direcciones creadas con 'admin', 'administrador', 'webmaster', 'hostmaster' o 'postmaster' como parte local, seguido del signo de arroba ("@"), seguido de un nombre de dominio de autorización,

    b. incluyendo un valor aleatorio en el correo electrónico, y

    c. hacer que el solicitante envíe (haciendo clic o de otra manera) el valor aleatorio a los servidores de Sectigo para confirmar la recepción y la autorización.

    El valor aleatorio, que es único, es generado por Sectigo y sigue siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su generación;

3. Hacer un cambio en el DNS según la sección 3.2.2.4.7 de los BRs del CAB Forum

   Confirmar el control del solicitante sobre el FQDN solicitado al confirmar la presencia de un valor aleatorio o token de solicitud en un registro CNAME de DNS o TXT para un nombre de dominio de autorización o un nombre de dominio de autorización que tiene como prefijo una etiqueta que comienza con un carácter de subrayado. El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación;

4. Gestión de la dirección IP según la sección 3.2.2.4.8 de los BRs del CAB Forum

   Confirmar el control del solicitante sobre el FQDN solicitado al confirmar que el solicitante controla una dirección IP devuelta de una búsqueda de DNS para registros A o AAAA para el FQDN.

   Este método no se usa para validación de dominios wildcard.

5. Enviar un email al contacto CAA de DNS según la sección 3.2.2.4.13 de los BRs del CAB Forum

   Confirmando el control del solicitante sobre el FQDN enviando un valor aleatorio por correo electrónico y luego recibiendo una respuesta de confirmación utilizando el valor aleatorio. El valor aleatorio debe enviarse a un contacto de correo electrónico de CAA de DNS. El conjunto de registros de recursos de CAA relevante se debe encontrar utilizando el algoritmo de búsqueda definido en RFC 8659 Sección 3.

   El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación

6. Enviar un email al contacto TXT de DNS según la sección 3.2.2.4.14 de los BRs del CAB Forum

   Confirmando el control del solicitante sobre el FQDN enviando un valor aleatorio por correo electrónico y luego recibiendo una respuesta de confirmación utilizando el valor aleatorio. El valor aleatorio debe enviarse a una dirección de correo electrónico identificada como un contacto de correo electrónico de registro TXT de DNS para el nombre de dominio de autorización seleccionado para validar el FQDN.

   El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación

7. Contacto telefónico con el contacto del dominio según la sección 3.2.2.4.15 de los BRs del CAB Forum.

   Confirmando el control del solicitante sobre el FQDN llamando al número de teléfono del contacto del dominio y obteniendo una confirmación para validar el AND.

En caso de que salte un contestador, Sectigo dejara un valor aleatorio y los ADNs que tienen que ser validados y recibir una confirmación usando el valor aleatorio.

El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación

8. Contacto telefónico con el teléfono del registro del DNS TXT según la sección 3.2.2.4.16 de los BRs del CAB Forum.

   Confirmando el control del solicitante sobre el FQDN llamando al número de teléfono del registro DNS TXT y obteniendo una confirmación para validar el AND.

   En caso de que salte un contestador, Sectigo dejara un valor aleatorio y los ADNs que tienen que ser validados y recibir una confirmación usando el valor aleatorio.

   El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación

9. Contacto telefónico con el contacto CAA del DNS según la sección 3.2.2.4.17 de los BRs del CAB Forum.

   Confirmar el control del Solicitante sobre el FQDN llamando al número de teléfono del contacto telefónico del DNS CAA y obtener una respuesta de confirmación para validar el ADN. El conjunto de registros de recursos CAA pertinente debe encontrarse utilizando el algoritmo de búsqueda definido en RFC 8659 Sección 3.

   En caso de que salte un contestador, Sectigo dejara un valor aleatorio y los ADNs que tienen que ser validados y recibir una confirmación usando el valor aleatorio.

   El valor aleatorio, que es único, es generado por Sectigo y permanece válido por no más de 30 días desde su generación.

10. Cambio acordado al sitio web v2 como se define en la sección 3.2.2.4.18 de los BRs del CAB Forum

    Confirmar el control del solicitante sobre el FQDN solicitado mediante la verificación de que el token de solicitud o el valor aleatorio se encuentran en el contenido de un archivo.

    Confirmar que el token de solicitud o el valor aleatorio se encuentra en el nombre de dominio de autorización, en HTTP[S]://<dominio de autorización>/.well-known/pki-validation/ a través del puerto 80 (HTTP) o 443 (HTTPS) .

    El Valor Aleatorio, que es único, es generado por Sectigo y permanece válido para su uso por no más de 30 días desde su generación.

    Este método no se utiliza para validar nombres de dominio wildcard

11. Cambio acordado en el sitio web – ACME como se define en la sección 3.2.2.4.19 de los BRs del CAB Forum.

    Confirmar el control del Solicitante sobre el FQDN mediante la validación del control de dominio del FQDN mediante el método ACME HTTP Challenge como se define en la sección 8.3 de RFC 8555.

    El token (como se define en la sección 8.3 del RFC 8555) es generado por Sectigo y sigue siendo válido para su uso durante no más de 30 días desde su generación.

    Este método no se utiliza para validar nombres de dominio wildcard

12. TLS usando ALPN como se define en la sección 3.2.2.4.20 de los BRs del CAB Forum.

    Confirmación del control del Solicitante sobre un FQDN mediante la validación del control de dominio del FQDN mediante la negociación de un nuevo protocolo de capa de aplicación mediante la Extensión de negociación de protocolo de capa de aplicación (ALPN) TLS [RFC7301] como se define en RFC 8737. El token (como se define en RFC 8737, inciso 3) NO SE UTILIZARÁ por más de 30 días desde su creación.

    Este método no se utiliza para validar nombres de dominio wildcard

3.2.3.1.2. Verificación de la dirección IP

Para cada dirección IP que se incluirá en un QWAC, Sectigo verifica el control de la IP por parte del solicitante de acuerdo con los Requisitos de referencia del CAB Forum, sección 3.2.2.5, utilizando uno de los siguientes métodos para cada IP

1. Cambio acordado en el sitio web como se define en la sección 3.2.2.5.1 de los BRs del CAB Forum

   Confirmar el control del solicitante sobre la dirección IP solicitada al confirmar la presencia de un token de solicitud o un valor aleatorio incluido en el contenido de un archivo o página web en forma de metaetiqueta en el directorio "/.well-known/pki-validation" , u otra ruta registrada con IANA con el fin de validar el control de las direcciones IP, en la dirección IP a la que puede acceder la CA a través de HTTP / HTTPS a través de un puerto autorizado. El token de solicitud o el valor aleatorio no aparecerán en la solicitud.

   Cuando se utiliza un valor aleatorio, que es único, permanece válido para su uso durante no más de 30 días desde su generación.

2. Contacto por correo electrónico, fax, SMS o correo postal a la dirección IP según se define en la sección 3.2.2.5.2 de los BRs del CAB Forum

   Confirmar el control del solicitante sobre la dirección IP enviando un valor aleatorio por correo electrónico, fax, SMS o correo postal y luego recibir una respuesta de confirmación utilizando el valor aleatorio. El valor aleatorio se enviará a una dirección de correo

electrónico, número de fax / SMS o dirección de correo postal identificada como un contacto de dirección IP. El valor aleatorio es único en cada correo electrónico, fax, SMS o correo postal.

El valor aleatorio sigue siendo válido para su uso en una respuesta de confirmación durante no más de 30 días desde su creación.

3. Búsqueda inversa de direcciones como se define en la sección 3.2.2.5.3 de los BRs del CAB Forum

   Confirmar el control del solicitante sobre la dirección IP mediante la obtención de un nombre de dominio asociado con la dirección IP a través de una búsqueda de IP inversa en la dirección IP y luego verificar el control sobre el FQDN utilizando un método permitido en la Sección 3.2.2.1.1 anterior.

4. Teléfono de contacto con dirección IP de contacto según se define en la sección 3.2.2.5.5 de los BRs del CAB Forum.

   Confirmar el control del Solicitante sobre la Dirección IP llamando al número de teléfono del contacto de la Dirección IP y obtener una respuesta de confirmación para validar la Dirección IP. Sectigo realiza la llamada a un número de teléfono identificado por la Autoridad de registro de direcciones IP como el contacto de la dirección IP.

   En caso de comunicarse con el correo de voz, Sectigo dejará un valor aleatorio y la dirección IP se validará y luego recibirá una respuesta de confirmación utilizando el valor aleatorio.

   El Valor Aleatorio, que es único, es generado por Sectigo y permanece vigente por no más de 30 días desde su generación.

5. Método “http-01” de ACME para direcciones IP según se define en la sección 3.2.2.5.6 de los BRs del CAB Forum.

   Confirmar el control del Solicitante sobre la dirección IP mediante la realización del procedimiento documentado para un desafío "http-01" en el borrador 04 de "Extensión de validación del identificador de IP de ACME", disponible en https://tools.ietf.org/html/draft-ietf -acme-ip-04#sección-4.

6. Método ACME “tls-alpn-01” para direcciones IP según se define en la sección 3.2.2.5.7 de los BRs del CAB Forum.

   Confirmar el control del Solicitante sobre la dirección IP mediante la realización del procedimiento documentado para un desafío "tls-alpn-01" en el borrador 04 de "ACME IP Identifier Validation Extension", disponible en https://tools.ietf.org/html/draft -ietf-acme-ip-04#sección-4.

3.2.4. PSD2

Los certificados PSD2 son certificados de persona jurídica que se pueden emitir como QWAC o como Sellos y, cuando están en Sellos, estos pueden emitirse en QSCD o no.

Estos certificados cumplen con la "Política de certificados cualificados de la UE emitidos a personas jurídicas" de ETSI: (QCP-l-qscd), (QCP-l), (QCP-w), (QCP-w-psd2).

3.2.4.1. Proceso de verificación de identidad

Pasos adicionales para verificar los atributos específicos de PSD2, incluido el nombre de la autoridad nacional competente (NCA), el número de autorización de PSD2 u otro identificador reconocido y las funciones de PSD2.

Estos detalles son proporcionados por el Solicitante del Certificado y confirmados por Sectigo utilizando información auténtica de la NCA (por ejemplo, utilizando un registro público nacional, Registro EBA PSD2, Registro de Instituciones de Crédito EBA o carta autenticada).

Sectigo también confirma la (s) función (es) PSD2 del solicitante del certificado (RolesOfPSP) de acuerdo con las reglas de validación proporcionadas por la NCA, si corresponde:

- servicio de cuenta (PSP_AS) OID: id-psd2-role-psp-as {0.4.0.19495.1.1}
- OID de inicio de pago (PSP_PI): id-psd2-role-psp-pi {0.4.0.19495.1.2}
- información de cuenta (PSP_AI) OID: id-psd2-role-psp-ai {0.4.0.19495.1.3}
- emisión de instrumentos de pago basados en tarjeta (PSP_IC) OID: id-psd2-role-psp-ic {0.4.0.19495.1.4}

Los certificados que requieren un QSCD cumplen los requisitos establecidos en el Anexo II del Reglamento eIDAS.

Las obligaciones del suscriptor (o, respectivamente, las obligaciones del TSP que administra la clave en su nombre) requieren que la clave privada se mantenga (o, respectivamente, se use) bajo el control exclusivo del sujeto.

3.2.5. Método para demostrar la posesión de la clave privada

Cuando Sectigo no genera la clave privada (es decir, QWAC), el medio habitual por el cual Sectigo acepta datos firmados de un solicitante para demostrar la posesión de una clave privada es al recibir una solicitud de firma de certificado (CSR) PKCS # 10.

La verificación de una firma digital se utiliza para determinar que:

- la clave privada correspondiente a la clave pública que figura en el certificado del firmante creó la firma digital, y
- los datos firmados asociados con esta firma digital no han sido alterados desde que se creó la firma digital.

3.2.6. Validación de autoridad

La validación de la autoridad implica la determinación de si una persona física tiene derechos o permisos específicos, incluido el permiso para actuar en nombre de una persona jurídica para obtener un certificado. La validación de la autoridad depende del tipo de certificado solicitado y se realiza de acuerdo con la sección 3.2 de esta DPC.

Para los certificados de persona jurídica, Sectigo utilizará un método de comunicación confiable para verificar la autenticidad de la solicitud de certificado del representante del solicitante.

Sectigo puede establecer la autenticidad de la solicitud de certificado directamente con el representante del solicitante, el representante autorizado de la persona física o de la persona jurídica o con una fuente autorizada dentro de la organización del solicitante.

Además, Sectigo establecerá un proceso que permita al solicitante especificar las personas físicas que pueden solicitar certificados. Si un solicitante especifica, por escrito, las personas físicas que pueden solicitar un certificado, Sectigo no aceptará ninguna solicitud de certificado que esté fuera de esta especificación. Sectigo proporcionará al solicitante una lista de sus solicitantes de certificados autorizados tras la solicitud por escrito verificada del solicitante.

Específicamente para los QWAC, la autorización del Registrante del Nombre de Dominio se verifica como se documenta en la sección 3.2.3.1 de esta DPC y esta solicitud se verifica de acuerdo con el documento del CA/B Forum para la Emisión y Gestión de Certificados de Validación Extendida sección 11.5.

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.

Todos los Certificados cruzados que identifican a una CA de Sectigo como Sujeto se enumeran en el Repositorio, siempre que Sectigo haya dispuesto o aceptado el establecimiento de la relación de confianza.

3.2.8. Validación de la solicitud

Antes de emitir un certificado, Sectigo emplea controles para validar la identidad de la información del suscriptor que aparece en la solicitud del certificado. Dichos controles son indicativos del tipo de producto.

3.3. Identificación y autenticación para solicitudes de renovación de claves

Sectigo admite cambios de clave en:

- Reemplazo, que es cuando un suscriptor desea cambiar algunos (o ninguno) de los detalles del sujeto en un certificado ya emitido y puede (o no) también desear cambiar la clave asociada con el nuevo certificado; y
- Renovación, que es cuando un suscriptor desea extender la vida útil de un certificado que ha sido emitido, al mismo tiempo puede variar algunos (o ninguno) de los detalles del sujeto y también puede cambiar la clave asociada con el certificado.

En ambos casos, Sectigo requiere que el suscriptor utilice los mismos detalles de autenticación que utilizó 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, el asunto debe volver a verificarse.

3.3.1. Identificación y autenticación para el cambio de clave

Como se indicó anteriormente, en ambos casos, Sectigo requiere que el suscriptor use los mismos detalles de autenticación que utilizó en la compra original del certificado.

3.3.2. Identificación y autenticación para la nueva generación de claves después de la revocación

Sectigo no permite de forma rutinaria la renovación de claves (o cualquier forma de reemisión o renovación) después de la revocación. La revocación es un evento terminal en el ciclo de vida del certificado.

Cuando se considera una solicitud de reemplazo o renovación de un certificado después de la revocación, Sectigo requiere que el suscriptor se autentique utilizando los detalles de autenticación originales utilizados en la compra inicial del certificado. Sin embargo, esto puede variar, o la reinscripción puede ser rechazada después de la revocación, cuando las circunstancias exactas y las razones por las cuales se revocó el certificado no se explican adecuadamente. La reemisión o reemplazo después de la revocación queda a criterio exclusivo de Sectigo.

3.4. Identificación y autenticación para solicitud de revocación

Revocación a solicitud del Suscriptor:

El Suscriptor debe estar en posesión de los detalles de autenticación (generalmente nombre de usuario y contraseña) para iniciar sesión en el sitio correspondiente que se utilizó para comprar el Certificado originalmente o el Suscriptor debe poder enviar un correo electrónico a nuestras cuentas de abuso que se autenticarán en una etapa posterior (por ejemplo, este correo electrónico se puede firmar con la Clave Privada asociada al 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 otras CA. Sectigo puede revocar, y lo hace, los certificados de suscriptor por la causa que se establece en la sección 4.9 de esta DPC, pero en estos casos no se requiere identificación y autenticación.

Sectigo emplea el siguiente procedimiento para autenticar una solicitud de revocación:

- La solicitud de revocación debe ser enviada por el contacto asociado con la solicitud de certificado. Sectigo también puede, si es necesario, solicitar que la solicitud de revocación sea realizada por el contacto de la organización y el contacto de facturación.
- Al recibir la solicitud de revocación, Sectigo solicitará la confirmación.
- El personal de validación de Sectigo ordenará la revocación del certificado y el registro de la identidad del personal de validación y el motivo de la revocación se mantendrá de acuerdo con los procedimientos de registro cubiertos en esta DPC.

4. REQUISITOS OPERACIONALES DEL CICLO DE VIDA DEL CERTIFICADO

Esta sección describe el proceso de solicitud de 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 cualificados de Sectigo varía según el tipo de certificado. Sectigo se reserva el derecho de, a su discreción, emitir certificados que pueden caer fuera de estos períodos establecidos.

Los siguientes pasos describen los principales hitos para emitir un certificado:

1. El solicitante completa la solicitud en línea en el sitio web de Sectigo y el solicitante envía la información requerida: Solicitud de firma de certificado (CSR) en caso de QWAC o aquellos no emitidos dentro de un QSCD, dirección de correo electrónico si es necesario, nombre común, información de la organización, código de país, método de verificación de identidad, información de facturación, etc.
2. El solicitante acepta el Acuerdo de suscripción en línea.
3. El solicitante envía la información requerida a Sectigo.
4. El solicitante paga las tarifas del certificado.
5. Sectigo identifica al solicitante, ya sea una persona física o jurídica, que será el sujeto del certificado y verifica la información enviada utilizando bases de datos de terceros y registros gubernamentales.
6. Tras la validación exitosa de la información de la solicitud, Sectigo puede emitir el certificado al solicitante o, si la solicitud es rechazada, Sectigo alertará al solicitante de que la solicitud no ha sido exitosa.
7. La renovación se realiza según los procedimientos descritos en esta DPC y los sitios web oficiales de Sectigo.
8. La revocación se lleva a cabo según los procedimientos descritos en esta DPC.

4.1. Solicitud de certificado

La solicitud de certificado se puede realizar de la siguiente manera:

Vía web. El solicitante del certificado envía una solicitud a través de un enlace seguro en línea de acuerdo con un procedimiento proporcionado por Sectigo. Es posible que se requiera documentación adicional en apoyo de la solicitud para que Sectigo verifique la identidad del solicitante. El solicitante presenta a Sectigo dicha documentación adicional. Tras la verificación de la identidad, Sectigo emite el certificado y envía una notificación al solicitante. El solicitante

debe notificar a Sectigo de cualquier inexactitud o defecto en un certificado inmediatamente después de recibir el certificado o notificación anterior del contenido informativo que se incluirá en el certificado.

Por correo electrónico: Sectigo puede, a su discreción, aceptar solicitudes por correo electrónico.

RA: Sectigo puede otorgar algunas RA para aceptar solicitudes a su discreción.

4.1.1. Quién puede enviar una solicitud de certificado

Generalmente, los solicitantes completarán los formularios en línea puestos a disposición por Sectigo o por las RA aprobados en los respectivos sitios web oficiales.

El solicitante, un representante o un RA en nombre del suscriptor deberá presentar una solicitud de certificado de suscriptor a la CA.

En circunstancias especiales, el solicitante puede enviar una solicitud por correo electrónico; sin embargo, este proceso está disponible a discreción de Sectigo o sus RA.

Sectigo mantiene una base de datos interna de todos los Certificados revocados anteriormente y las solicitudes de certificados rechazadas anteriormente. Esa base de datos se utiliza para identificar solicitudes de certificados sospechosas posteriores.

4.1.1.1. Solicitudes de certificado de socio revendedor

Los Socios revendedores pueden actuar como RA según las prácticas y políticas establecidas en esta DPC. La RA puede realizar la solicitud en nombre del solicitante de conformidad con el programa de revendedor.

En tales circunstancias, la RA es responsable de todas las funciones en nombre del solicitante detalladas en la sección 4.1.2 de esta DPC. Dichas responsabilidades se detallan y mantienen dentro del acuerdo y las pautas del revendedor de alojamiento web.

4.1.2. Proceso de inscripción y responsabilidades

Todos los solicitantes de certificados deben completar el proceso de inscripción, que puede incluir:

- Generar un par de claves RSA o ECC y demuestre a Sectigo la propiedad de la clave privada asociada con la clave pública que se incluirá en el certificado mediante el envío de una solicitud de firma de certificado (CSR) PKCS # 10 válida en el caso de QWAC o de aquellos que no sean emitidos dentro de un token. Para los emitidos en dispositivos, los pares de claves son generados por Sectigo y luego entregan de forma segura ese dispositivo al solicitante, con la diferencia de los HSM en donde no existe tal entrega específica.
- Hacer todos los esfuerzos razonables para proteger la integridad y confidencialidad de la clave privada.

- Enviar a Sectigo una solicitud de certificado, incluida la información de la solicitud como se detalla en esta DPC y acepte los términos del Acuerdo de suscripción correspondiente.
- Aportar prueba de identidad mediante la presentación de la documentación oficial solicitada por Sectigo durante el proceso de inscripción.

4.2. Procesamiento de solicitud de certificado

Las solicitudes de certificado se envían a Sectigo o a una RA aprobada por Sectigo. La siguiente tabla detalla las entidades involucradas en el procesamiento de las solicitudes de certificados. Sectigo emite todos los certificados independientemente de la entidad procesadora.

Tipo de certificado	Entidad de inscripción	Entidad de procesamiento	Autoridad emisora
Certificado cualificado para persona física	Usuario final o suscriptor de entidad	Sectigo o suscriptor de entidad	Sectigo
Certificado cualificado para persona jurídica	Suscriptor de la entidad	Sectigo	Sectigo
Certificado cualificado para sitios web	Usuario final o suscriptor de entidad	Sectigo	Sectigo

4.2.1. Realización de funciones de identificación y autenticación

Al recibir una solicitud para un certificado cualificado y en base a la información enviada, Sectigo confirma la siguiente información:

- El solicitante del certificado es la misma persona que la identificada en la solicitud del certificado.
- La información que se publicará en el certificado es precisa, excepto la información del Suscriptor no verificada.
- Cualquier agente que solicite un certificado que incluya la clave pública del solicitante del certificado está debidamente autorizado para hacerlo.

Sectigo puede utilizar los servicios de un tercero para confirmar la información de una persona física o jurídica que solicita un certificado cualificado. Sectigo acepta la confirmación de organizaciones de terceros, otras bases de datos de terceros y entidades gubernamentales.

Los controles de Sectigo también pueden incluir transcripciones de registros comerciales que confirmen el registro de la empresa solicitante y mencionen los miembros de la junta, la administración y los directores que representan a la empresa.

Sectigo podrá utilizar cualquier medio de comunicación a su alcance para conocer la identidad de una persona física o jurídica solicitante. Sectigo se reserva el derecho de rechazo a su absoluta discreción.

Para los QWAC, Sectigo tiene un sistema implementado que examina los detalles del sujeto, incluidos los nombres de dominio, en busca de coincidencias o casi coincidencias con algunos nombres conocidos de alto perfil o notificados previamente que pueden indicar que un certificado tiene un riesgo más alto de lo normal de que las aplicaciones fraudulentas sean realizado y, en esos casos, la solicitud de certificado se marca para revisión manual.

4.2.2. Aprobación o rechazo de solicitudes de certificado

Después de completar con éxito todas las validaciones requeridas de una solicitud de certificado, Sectigo aprueba una solicitud de certificado digital.

Si falla la validación de una solicitud de certificado, Sectigo rechaza la solicitud de certificado. Sectigo se reserva el derecho de rechazar solicitudes para emitir un certificado a los solicitantes si, según su propia evaluación, al emitir un certificado a dichas partes, el nombre de Sectigo podría empañarse, disminuir o reducir su valor y, en tales circunstancias, podría hacerlo así sin incurrir en responsabilidad alguna por cualquier pérdida o gasto que surja como resultado de dicha negativa.

Los solicitantes cuyas solicitudes hayan sido rechazadas pueden volver a presentar una solicitud posteriormente.

En 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 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 bajo el Acuerdo de Suscriptor.

4.2.3. Tiempo de procesamiento de las solicitudes de certificados

Sectigo realiza esfuerzos razonables para confirmar la información de la solicitud de certificado y emitir un certificado digital dentro de un período razonable. El período depende en gran medida de que el Suscriptor proporcione los detalles y / o documentación necesarios de manera oportuna. Una vez recibidos los detalles y / o la documentación necesarios, Sectigo tiene como objetivo confirmar los datos de la solicitud enviada y completar el proceso de validación y emitir / rechazar una solicitud de certificado en un plazo de 2 días hábiles.

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 (solo para QWAC)

Cuando una solicitud es para un QWAC, Sectigo examina los Registros de recursos DNS de Autorización de la autoridad de certificación (CAA) según se especifica en RFC 8659 y, si dichos

Registros CAA están presentes y no otorgan a Sectigo la autoridad para emitir el certificado, la solicitud es rechazada. Sectigo registra todos los logs de los resultados de las comprobaciones de CAA.

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 por parte de Sectigo.

- 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

Sectigo emite un certificado tras la aprobación de una solicitud de certificado. Un certificado cualificado se considera válido en el momento en que un Suscriptor lo acepta (consulte la sección 4.4 de esta DPC). Emitir un certificado cualificado significa que Sectigo acepta una solicitud de certificado.

Los certificados cualificados de Sectigo se expiden a organizaciones (personas jurídicas) o personas físicas (personas naturales).

Los suscriptores serán los únicos responsables de la legalidad de la información que presenten para su uso en los certificados emitidos bajo esta DPC, en cualquier jurisdicción en la que dicho contenido pueda ser usado o visto.

4.3.1. Acciones de CA durante la emisión del certificado

Los sistemas automatizados de Sectigo reciben y recopilan:

- evidencia recopilada durante el proceso de verificación, y / o
- afirmaciones de 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, un ejemplo de lo cual es un proceso de venta que involucra un pago con tarjeta de crédito.

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 externas 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.

Los únicos certificados que emite Sectigo de sus CA raíz son los certificados de CA intermedios y los certificados cruzados. Nuestra CA no tiene la capacidad para la firma automatizada de dichos certificados ni tampoco la firma/emisión de CRLs/OCSPs por sus root CAs correspondientes, por lo que esta actividad implica necesariamente la intervención manual de usuarios privilegiados para firmar dichos certificados/CRLs/OCSPs. La emisión de certificados por parte de la CA raíz requiere que una persona autorizada por la CA (es decir, el operador del sistema de CA, el oficial del sistema o el administrador de PKI) emita deliberadamente un comando directo para que la CA raíz realice una operación de firma de certificado.

Los sistemas de emisión de Sectigo:

- no actualizan hacia atrás las fechas notBefore para evitar plazos, prohibiciones o restricciones
- cuentan con mecanismos previos y posteriores a la emisión para reducir las posibles emisiones erróneas que puedan ocurrir. El uso de herramientas de tipo “linting” ayuda a lograr este objetivo.
    - Para los certificados QWAC, Sectigo realiza una emisión previa a la emisión utilizando ZLint, CABLint y x509lint.
- proporcionan servicios OCSP para certificados que se supone que existen en función de un precertificado existente, incluida la capacidad de revocar dicho certificado.

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

Sectigo notifica al suscriptor de la emisión de un certificado cualificado, ya sea por correo electrónico y / o mediante entrega. La entrega de certificados de suscriptor al suscriptor asociado depende de quién genera los pares de claves y el dispositivo utilizado:

Certificados cualificados para persona física y jurídica emitidos dentro de un dispositivo (QSCD o no QSCD)

La notificación de la emisión de estos certificados se envía por correo electrónico al Suscriptor utilizando la dirección de correo electrónico de contacto proporcionada durante el proceso de solicitud. El certificado se entregará al suscriptor mediante un método confiable y seguro, generalmente por mensajería.

Certificados cualificados para persona física y jurídica no emitidos dentro de un dispositivo

Tras la emisión de estos certificados cualificados, el suscriptor recibe por correo electrónico un enlace de recopilación utilizando el correo electrónico proporcionado

durante la solicitud. El suscriptor debe visitar el enlace de recopilación utilizando el mismo ordenador desde el que se realizó la solicitud del certificado original. El software del proveedor de servicios criptográficos del suscriptor se inicia para garantizar que el suscriptor posea la clave privada correspondiente a la clave pública enviada durante la solicitud. En espera de un desafío exitoso, el certificado emitido se instala automáticamente en la computadora del Suscriptor. Otra opción es entregar el certificado directamente por correo electrónico al suscriptor utilizando la dirección de correo electrónico de contacto del administrador proporcionada durante el proceso de solicitud.

4.3.3. Negativa 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.

4.4.1. Conducta que constituye la aceptación del certificado

Un certificado emitido se envía por correo electrónico o se instala en el módulo de seguridad del ordenador/hardware del Suscriptor a través de un método de recolección en línea. Se considera que un suscriptor ha aceptado un certificado cuando:

- el suscriptor usa el certificado, o
- Pasan 30 días desde la fecha de emisión de un certificado.

4.4.2. Publicación del certificado por la CA

Un certificado se publica a través de varios medios:

- por Sectigo poniendo el certificado a disposición en el Repositorio; y
- por el Suscriptor utilizando 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

Aparte del Suscriptor, Sectigo proporciona notificación de la emisión del certificado a otras entidades determinadas como se detalla a continuación.

4.4.3.1. Socio revendedor

Los QWAC de suscriptor emitidos solicitados a través de un socio revendedor en nombre del suscriptor se envían por correo electrónico al contacto del administrador de la cuenta del socio revendedor del host web. Para los Socios revendedores que utilizan la interfaz de "aplicación automática", los revendedores tienen la opción adicional de recopilar un certificado emitido de una URL específica de la cuenta de revendedor.

4.5. Par de claves y uso de certificados

Esta sección se utiliza para describir las responsabilidades relacionadas con el uso de claves y 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 de parte de confianza

La decisión final sobre si confiar o no en una firma/sello avanzado/cualificado es exclusivamente del tercero de confianza. La confianza en una firma/sello cualificado/avanzado solo debe ocurrir si:

- la firma/ sello se creó durante el período operativo de un certificado válido y se puede verificar haciendo referencia a un certificado validado;
- el tercero de confianza ha verificado el estado de revocación del certificado haciendo referencia a las CRL pertinentes y el certificado no ha sido revocado;
- el tercero de confianza ha verificado con el TSL correspondiente;
- el tercero de confianza entiende que se emite un certificado cualificado a un suscriptor para un propósito específico y que el certificado cualificado solo puede usarse de acuerdo con los usos sugeridos en esta DPC y nombrados como Identificadores de Objeto en el perfil del certificado; y
- el certificado solicitado es apropiado para la aplicación en la que se utiliza.

La confianza se acepta como razonable según las disposiciones hechas para el tercero de confianza bajo esta DPC y dentro del acuerdo entre ambas partes. Si las circunstancias de la confianza exceden las garantías entregadas por Sectigo bajo las disposiciones de esta DPC, el tercero de confianza debe obtener garantías adicionales.

Las garantías solo son válidas si se han realizado los pasos detallados anteriormente.

4.6. Renovación de 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.

Dependiendo de la opción seleccionada durante la aplicación, el período de validez de los certificados de Sectigo se detalla en el campo correspondiente dentro del certificado.

Las tarifas de renovación se detallan en los sitios web oficiales de Sectigo y en las comunicaciones enviadas a los Suscriptores que se acercan a la fecha de vencimiento del certificado.

4.6.1. Circunstancia para la renovación del certificado

Sectigo hará todos los esfuerzos razonables para notificar a los suscriptores por correo electrónico la inminente caducidad de un certificado digital. Por lo general, la notificación se proporcionará dentro de un período de 60 días antes de la expiración del certificado.

4.6.2. Quién puede solicitar la renovación

Aquellos que pueden solicitar la renovación de un certificado incluyen, entre otros, un suscriptor en nombre de sí mismo y un RA en nombre de un suscriptor. Sectigo no renueva certificados automáticamente.

4.6.3. Procesamiento de solicitudes de renovación de certificados

Para procesar las solicitudes de renovación de certificados, Sectigo hace que el suscriptor se vuelva a autenticar. Los requisitos y procedimientos de la solicitud de renovación son los mismos que los empleados para la validación de la solicitud y los requisitos de emisión detallados para nuevos clientes, pero verificando que el material criptográfico aún sea suficiente para el nuevo certificado y que no haya indicios de que la clave privada del sujeto haya ha sido comprometido ni el certificado ha sido revocado debido a una violación de seguridad.

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

La notificación al suscriptor sobre la emisión de un certificado renovado se da por los mismos medios que un nuevo certificado, descrito en el apartado 4.3.2 de esta DPC.

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

La conducta del suscriptor que constituye la aceptación de un certificado de renovación es la misma que se enumera en la sección 4.4.1 de esta DPC.

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

Sectigo publica un certificado renovado entregándolo al suscriptor. En las circunstancias limitadas en las que Sectigo publica un certificado renovado por medios alternativos, Sectigo lo hace utilizando el servidor LDAP, un directorio de certificados de cliente de acceso público.

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

Generalmente, Sectigo no notifica a otras entidades sobre un certificado renovado. En circunstancias limitadas, Sectigo notificará a otras entidades a través de los medios descritos en la sección 4.6.6 de esta DPC. Sectigo también puede notificar a una RA, si la RA estuvo involucrada en el proceso de renovación.

4.7. Cambio de clave de un certificado

La sección se utiliza para describir elementos / procedimientos que generan un nuevo par de claves y solicitan la emisión de un nuevo certificado que certifica la nueva clave pública. Volver a emitir un certificado puede comprender la creación de un nuevo certificado con una nueva clave pública y número de serie, conservando la información del asunto del certificado.

4.7.1. Circunstancias para la renovación de claves del certificado

El cambio de clave del certificado se llevará a cabo normalmente como parte de la renovación o reemplazo de un certificado, como se indica en la sección 3.2 de esta DPC. La renovación de la clave del certificado también puede tener lugar cuando una clave se ha visto comprometida.

4.7.2. Quién puede solicitar el cambio de clave del certificado

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 renovación de claves de certificados

Dependiendo de las circunstancias, el procedimiento para procesar una nueva clave de certificado puede ser el mismo que para emitir un nuevo certificado. En otras circunstancias, Sectigo puede procesar una solicitud de cambio de clave haciendo que el suscriptor autentique su identidad.

4.7.4. Notificación de cambio de clave al suscriptor

Sectigo notificará al suscriptor de un cambio de clave de certificado por los medios delineados en la sección 4.3.2 de esta DPC.

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

La conducta del suscriptor que constituye la aceptación de un certificado con clave modificada es la misma que se enumera en la sección 4.4.1 de esta DPC.

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

La publicación de un certificado con clave nueva se realiza entregándolo al suscriptor.

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

Generalmente, Sectigo no notifica a otras entidades sobre la emisión de un certificado con clave nueva. Sectigo puede notificar a un RA de la emisión de un certificado con clave nueva cuando un RA estuvo involucrado en el proceso de emisión.

4.8. Modificación de un certificado

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

4.9. Revocación y suspensión de certificados

La revocación de un certificado es terminar permanentemente el período operativo del certificado antes de llegar al final de su período de validez establecido. En otras palabras, tras la revocación de un certificado, el período operativo de ese certificado se considera inmediatamente terminado. El número de serie del certificado revocado se colocará dentro de la CRL y permanecerá en la CRL como se indica en la sección 4.9.7. Sectigo informa al sujeto del certificado o a los suscriptores del cambio de estado del certificado.

Sectigo no utiliza la suspensión de certificados.

4.9.1. Circunstancias para la revocación

Sectigo revocará un certificado dentro de las 24 horas posteriores a la recepción de la solicitud de revocación si ocurre una o más de las siguientes situaciones:

- El Suscriptor solicita por escrito que la CA revoque el certificado;
- El Suscriptor notifica a Sectigo que la solicitud de certificado original no fue autorizada y no otorga la autorización retroactivamente;
- Sectigo cree razonablemente que ha habido pérdida, robo, modificación, divulgación no autorizada u otro compromiso de la clave privada asociada con el certificado;
- Se informa a Sectigo de un método demostrado o probado que puede calcular fácilmente la clave privada del suscriptor en función de la clave pública en el certificado (como una clave débil de Debian, consulte https://wiki.debian.org/SSLkeys);

- El Suscriptor o Sectigo ha incumplido una obligación material en virtud de esta DPC o del Acuerdo de Suscriptor correspondiente;
- Las obligaciones del Suscriptor o de Sectigo en virtud de esta DPC o el Acuerdo de Suscriptor correspondiente se retrasan o se evitan por un desastre natural, fallo en los ordenadores o en las comunicaciones, u otra causa más allá 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;
- Sectigo tiene conocimiento de un cambio sustancial en la información contenida en el certificado, o la información contenida en el certificado es inexacta;
- Un número de identificación personal, clave privada o contraseña ha sido 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.
- El certificado no ha sido emitido de acuerdo con las políticas establecidas en esta DPC;
- El Suscriptor ha utilizado el certificado 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 fue emitido a personas o entidades identificadas como editores de software malintencionado o que se hizo pasar por otras personas o entidades;
- El certificado fue emitido como resultado de fraude o negligencia;
- Sectigo tiene conocimiento 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, o si hay evidencia clara de que el método específico utilizado para generar la clave privada fue defectuoso;
- El derecho de Sectigo a emitir certificados vence o se revoca o termina, a menos que Sectigo haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;
- El Precertificado y el Certificado no coinciden exactamente entre sí según RFC 6962;
- 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 CA subordinada no se emitió de acuerdo con esta DPC o que la CA subordinada no ha cumplido con ella;

- 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 bajo los Requisitos básicos (BR) expira o es revocado o terminado, a menos que Sectigo haya hecho arreglos para continuar manteniendo el Repositorio de CRL / OCSP;
- Esta DPC 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 se emitió a personas o entidades identificadas como editores de software malintencionado 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

Un suscriptor u otra parte debidamente autorizada puede solicitar la revocación de un certificado. Una parte autorizada incluye una RA, independientemente de si en nombre del suscriptor puede solicitar la revocación a través de su cuenta. Sectigo puede revocar un certificado sin recibir una petición de revocación y sin ninguna otra razón. Otras partes pueden reportar sospechas de Compromiso de la Clave Privada, uso indebido de certificados u otros tipos de fraude, compromiso, uso indebido, 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 del apartado 3.4 de esta DPC.

4.9.4. Tiempo dentro del cual Sectigo procesará la solicitud de revocación

Sectigo procesará las solicitudes de revocación de acuerdo con esta DPC. 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

Las partes que confían en un certificado cualificado deben verificar una firma digital en todo momento verificando la validez de un certificado digital con la CRL relevante publicada por Sectigo o utilizando el respondedor Sectigo OCSP. Hay que tener en cuenta que la CRL puede retrasarse con respecto a OCSP, lo que crea una situación en la que un certificado revocado se muestra como revocado en OCSP pero puede que no se muestre como revocado en la CRL más reciente disponible. Por lo tanto, se recomienda obtener información de revocación del respondedor OCSP de Sectigo siempre que sea posible. Se advierte a las partes que confían que no se puede asignar una firma digital no verificada como una firma válida del Suscriptor.

Por medio de esta DPC, Sectigo ha informado adecuadamente a los terceros de confianza sobre el uso y validación de firmas digitales a través de esta DPC y otra documentación publicada en el Repositorio como se especifica en la sección de Control de Documentos de este DPC.

4.9.6. Frecuencia de emisión de CRL

Para conocer el estado de los certificados de suscriptor:

Sectigo publica CRL para permitir que las partes confiantes verifiquen una firma digital realizada con un certificado digital emitido por Sectigo. Cada CRL contiene entradas para todos los certificados emitidos no vencidos revocados. Sectigo emite una nueva CRL cada 24 horas de forma predeterminada o en un plazo de 6 horas si se ha revocado un certificado. Todas las CRL vencidas se archivan (como se describe en la sección 3.4 de esta DPC) por un período de 15 años o más si corresponde. Para los certificados cualificados revocados, Sectigo mantendrá la información del certificado en las CRL durante al menos 10 años.

Para conocer el estado de los certificados de CA:

Sectigo actualizará y volverá a emitir las CRL al menos:

- una vez cada doce meses
- dentro de las 24 horas posteriores a la revocación de un certificado de CA, y el valor del campo nextUpdate no debe ser más de doce meses más allá del valor del campo thisUpdate
- dentro de las 24 horas posteriores a la expiración de un certificado de CA
- cada 30 días si Sectigo certifica esta jerarquía con un TSP de terceros

4.9.7. Latencia máxima para las CRL

La latencia máxima para las CRL significa el tiempo máximo entre la generación de las CRL y la publicación de las CRL en el repositorio (es decir, la cantidad máxima de demoras relacionadas con el procesamiento y la comunicación en la publicación de las CRL en el repositorio una vez generadas las CRL). Sectigo no emplea una latencia máxima para las CRL. Sin embargo, generalmente, las CRL se publican en 1 hora.

4.9.8. Disponibilidad de verificación de estado / revocación en línea

Además, los sistemas de Sectigo están configurados para generar y servir respuestas OCSP. Esto proporciona información en tiempo real sobre la validez del certificado haciendo que la información de revocación esté disponible inmediatamente a través del protocolo OCSP. Las CRL y OSCP están disponibles las 24 horas del día, los 7 días de la semana para cualquier persona.

El OCSP de Sectigo cumple con los estándares RFC 6960 y/o 5019.

4.9.9. Requisitos de verificación de revocación en línea

Las respuestas OCSP de Sectigo son:

- Firmado por la CA que emitió los certificados cuyo estado de revocación se está verificando, o;
- La respuesta OCSP está firmada por un certificado de respuesta OCSP separado que está firmado por la CA que emitió el certificado cuyo estado de revocación se está verificando. En este caso, el certificado de firma contendrá una extensión de tipo id-pkix-ocsp-nocheck, como se define en RFC6960.

Para conocer el estado de los certificados de suscriptor:

Todas las respuestas OCSP de Sectigo deben:

1. tener un intervalo de validez mayor o igual a ocho horas;

2. tener un intervalo de vigencia menor o igual a siete días;

3. actualizar la información proporcionada a través de OCSP antes de la mitad del período de validez antes de la próxima actualización.

Si el respondedor OCSP recibe una solicitud de estado de un certificado que no ha sido emitido, entonces el respondedor no responde con un estado "bueno". El TSP monitoriza al respondedor para tales solicitudes como parte de sus procedimientos de seguridad.

Para conocer el estado de los certificados de CA subordinada:

Sectigo actualizará esta información proporcionada a través de un Protocolo de estado de certificado en línea al menos:

- cada doce meses
- dentro de las 24 horas posteriores a la revocación de un certificado de CA subordinada.
- dentro de las 24 horas posteriores a la expiración de un certificado de CA

El respondedor OCSP puede proporcionar respuestas definitivas sobre números de serie de certificados "reservados", como si hubiera un Certificado correspondiente que coincidiera con

el Precertificado como se establece en RFC 6962. Un número de serie de certificado dentro de una solicitud OCSP es una de las siguientes tres opciones:

1. “asignado” si la CA Emisora ha emitido un Certificado con ese número de serie, utilizando cualquier clave actual o anterior asociada con el sujeto de esa CA; o

2. “reservado” si un Precertificado con ese número de serie ha sido emitido por

    - la CA Emisora; o
    - un Certificado de firma de precertificado asociado con la CA emisora; o

3. “sin usar” si no se cumple ninguna de las condiciones anteriores.

Los terceros de confianza deben realizar verificaciones de estado / revocación en línea de acuerdo con la sección 4.9.6 de esta DPC antes de confiar en el certificado.

4.10. Servicios de estado de certificados

CRL y OCSP son servicios de verificación del estado de los certificados disponibles para los terceros de confianza.

La información sobre el estado de la revocación está disponible más allá del período de validez del certificado

4.10.1. Características operativas

Sectigo ofrece un OCSP ligero que cumple con el RFC 5019. Sectigo proporciona información de revocación para certificados cualificados después de la fecha de vencimiento.

4.10.2. Servicio disponible

Los servicios de estado de certificados están disponibles 24 horas al día, 7 días a la semana.

4.11. Fin de suscripción

El servicio de suscripción de un suscriptor finaliza si

- Sectigo deja de funcionar,
- Todos los certificados de Suscriptor emitidos por Sectigo se revocan sin la renovación del certificado o renovación de claves de los certificados, o
- El Acuerdo de suscripción del suscriptor finaliza o vence sin renovación.

4.12. Depósito y recuperación de claves

Sectigo no proporciona custodia de claves ni servicios de copia de seguridad de claves.

5. CONTROLES OPERATIVOS, DE GESTIÓN Y DE INSTALACIONES

Esta sección describe la política de seguridad, los mecanismos de control de acceso físico, los niveles de servicio y la política de personal en uso para proporcionar operaciones de CA confiables.

Sectigo afirma que hace todos los esfuerzos razonables para detectar y prevenir infracciones materiales, pérdida, daño o compromiso de activos e interrupción de las actividades comerciales.

5.1. Controles físicos

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

5.1.1. Ubicación y construcción del sitio (CPD)

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

5.1.2. Acceso físico

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. Toda entrada al área físicamente segura de una persona no autorizada deberá estar acompañada por una persona autorizada mientras se encuentre en el área segura.

5.1.3. Energía y aire acondicionado

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

5.1.4. Exposiciones al agua

Sectigo ha realizado esfuerzos razonables para garantizar que sus instalaciones seguras estén protegidas de inundaciones y daños por agua. Sectigo tiene personal ubicado en el lugar para

reducir el alcance de los daños causados por una inundación y cualquier exposición posterior al agua.

5.1.5. Prevención y protección contra incendios

Sectigo ha realizado esfuerzos razonables para garantizar que sus instalaciones seguras estén protegidas del daño por fuego y humo (la protección contra incendios se realiza de acuerdo con las regulaciones locales contra incendios). El equipo de TI está ubicado para reducir el riesgo de daños o pérdidas por incendio. El nivel de protección contra incendios refleja la importancia del equipo.

5.1.6. Almacén de datos

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

5.1.7. Depósito de basura

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

5.1.8. Copia de seguridad fuera del sitio

Sectigo hace una copia de seguridad de su información en una ubicación segura fuera del sitio que está lo suficientemente distante para escapar de los daños de un desastre en la ubicación principal. El equipo de infraestructura determina la frecuencia, la retención y el alcance de la copia de seguridad, teniendo en cuenta los requisitos de criticidad y seguridad de la información. 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 debidamente etiquetados de acuerdo con la confidencialidad de la información.

5.2. Controles de procedimiento

5.2.1. Roles de confianza

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

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 la PKI de Sectigo. Todo el personal en funciones de confianza debe estar libre de conflictos de intereses que puedan perjudicar la imparcialidad de las operaciones de la PKI cualificada de Sectigo.

Las personas que actúan en roles de confianza solo pueden acceder a un CMS después de que se autentiquen mediante un método aprobado como adecuado

5.2.1.1. Administradores de CA

El administrador de CA instala y configura el software de 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 CA no emiten certificados a los suscriptores.

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

El rol de Oficial de 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 esta DPC, y el registro de los detalles de los pasos de aprobación y emisión realizados, las tareas de verificación de identidad se completan.

Los oficiales de 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 digital.

Existe un rol específico para los QWAC cuando actúan como especialistas en validación como se indica en las BR.

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 una RA están operando de acuerdo con esta DPC.

5.2.2. Número de personas necesarias por tarea

Sectigo requiere que al menos dos administradores de CA actúen para activar las claves privadas de CA de Sectigo para la firma, generar nuevos pares de claves de CA o restaurar claves privadas.

5.2.3. Identificación y autenticación para cada rol

Se requiere que todo el personal se autentique ante los sistemas CA y RA antes de que puedan desempeñar las funciones de su función en relación con esos sistemas.

Las claves privadas de CA solo pueden ser respaldadas, almacenadas y recuperadas por personal en roles de confianza utilizando, al menos, control dual en un entorno físicamente seguro.

5.3. Controles de personal

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

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

5.3.1. Requisitos de calificaciones, experiencia y autorización

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

- 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 / administrador de sistemas o el director ejecutivo.
- Los nuevos administradores son supervisados de cerca por el Administrador / 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. Este período de capacitación debe ser de al menos seis meses antes de que se otorguen privilegios de emisión para certificados cualificados.

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 seguridad 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.

- Los administradores de CA están capacitados en el funcionamiento e instalación del software de CA.
- Los operadores están capacitados en el mantenimiento, la configuración y el uso del software, los sistemas operativos y los sistemas de hardware específicos utilizados por 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 oficiales de CA están capacitados en las políticas y procedimientos de validación y verificación de Sectigo. Se requiere que pasen un examen con los requisitos de verificación y toda la información de la validación necesaria

Sectigo mantiene registros con toda la formación recibida por parte de los empleados.

5.3.4. Frecuencia y requisitos de formación

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

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 una falla o deficiencia en la capacitación, se realizará la formación suficiente para rectificar la deficiencia.

5.3.6. Requisitos del contratista independiente

Los contratistas independientes deben cumplir con los mismos requisitos de capacitación que los empleados de Sectigo que trabajan en el mismo rol.

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

5.3.7. Documentación suministrada al personal

La selección de la documentación suministrada al personal de Sectigo se basa en los roles que deben desempeñar. Dicha documentación puede incluir una copia de esta DPC, el reglamento eIDAS, los Requisitos de referencia del CAB Forum, las Directrices EV y otra documentación técnica y operativa necesaria para mantener las operaciones de la CA de Sectigo.

5.4. Procedimientos de registro de auditoría

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

5.4.1. Tipos de eventos registrados

Se mantiene un registro de auditoría de cada movimiento.

CA y eventos de gestión del ciclo de vida del certificado:

- Funciones clave de firma de las CAs, incluida la generación, copia de seguridad, recuperación y destrucción de claves
- Gestión del ciclo de vida de los certificados de suscriptor, incluidas las solicitudes de certificados satisfactorias y no satisfactorias, las emisiones de certificados, las reemisiones de certificados y las renovaciones de certificados.
- 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 portadores de claves
- Clave privada comprometida

Eventos relacionados con la seguridad:

- Tiempo de inactividad del sistema, fallos de software y de hardware y actividades de los routers y firewalls

- Arranque y parada de las funciones de logging
- Acciones del sistema de CA realizadas por el personal de Sectigo, incluidas actualizaciones de software, reemplazos de hardware y actualizaciones
- Eventos de QSCD (por ejemplo, HSM o tokens USB), como uso, desinstalación, servicio o reparación y retiro
- Intentos de acceso a la PKI de servicios cualificados con éxito y sin éxito
- Entrada y salida segura de visitantes a 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
- Identidad de la entidad que realiza la entrada del registro

5.4.2. Registro de frecuencia de procesamiento

El administrador del sistema archiva los registros y los 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 conservarán durante un mínimo de 2 años.

Esos son:

- Registros de eventos de gestión del ciclo de vida de claves y certificados de CA (como se establece en la Sección 5.4.1) después de la ocurrencia posterior de:

  - la destrucción de la clave privada de CA; o

  - la revocación o vencimiento del Certificado de CA final en ese conjunto de Certificados que tienen una extensión X.509v3 basicConstraints con el campo cA establecido en verdadero y que comparten una Clave pública común correspondiente a la Clave privada de CA;

- Registros de eventos de gestión del ciclo de vida del Certificado de Suscriptor (como se establece en la Sección 5.4.1) después de la revocación o vencimiento del Certificado de Suscriptor.
- Cualquier registro de eventos de seguridad (como se establece en la Sección 5.4.1) después de que ocurrió el evento.

5.4.4. Protección del registro de auditoría

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 respaldan en servidores locales separados y se transfieren fuera del sitio a través de una VPN encriptada a servidores remotos.

5.4.6. Sistema de recopilación de auditorías (interno frente a 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 y/o Administradores de 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 y/o humanas.

Los análisis de vulnerabilidades se ejecutan automáticamente con una programación trimestral. Se ejecutan exploraciones adicionales después de las actualizaciones del sistema, los cambios o cuando se considera necesario.

Sectigo realiza evaluaciones de riesgo anuales que identifican y evalúan amenazas internas y externas razonablemente previsibles que podrían resultar en acceso no autorizado, divulgación, uso indebido, alteración o destrucción de cualquier dato de los certificados o proceso de emisión de los certificados.

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

5.5. Archivo de registros

Sectigo implementa un estándar de respaldo para todos los sistemas críticos para el negocio ubicados en sus centros de datos. Sectigo conserva los registros en formato electrónico o en papel de conformidad con esta subsección de esta DPC.

5.5.1. Tipos de registros archivados

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

- Datos de auditoría, según se especifica en la sección 5.4 de esta DPC;
- 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 toda la documentación relacionada con las solicitudes de certificados y la verificación de las mismas, y todos los certificados y su revocación por un período no inferior a 15 años después de que cualquier certificado basado en esa documentación deje de ser válido, 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.

5.5.3. Protección de archivo

Los registros se archivan en una ubicación segura fuera del sitio 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

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 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
- Revocación de certificado

5.5.6. Sistema de recopilación 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 presenten la documentación adecuada para respaldar una solicitud de certificado.

Como parte de los procedimientos de recopilación externos de Sectigo, las RA pueden requerir documentación de los Suscriptores para respaldar las solicitudes de certificados, en su función de RA. En tales circunstancias, las RA están obligadas a conservar dichos registros de acuerdo con las prácticas de retención y protección de registros utilizadas por Sectigo y según lo establecido en esta DPC.

5.5.7. Procedimientos para obtener y verificar información de archivo

Se requiere que las RA externas de Sectigo presenten la documentación apropiada como se detalla en el acuerdo de socio revendedor de alojamiento web, y antes de ser validados y aceptados con éxito como RA aprobado por Sectigo.

5.6. Cambio de clave

Hacia el final de la vida útil de cada raíz o subCA, se encarga un nuevo par de claves de firma de CA y todos los certificados y CRL emitidos posteriormente se firman con la nueva clave de firma privada. Ambas claves pueden estar activas al mismo tiempo. El nuevo certificado de clave pública de CA correspondiente se proporciona a los suscriptores y terceros de confianza a través de los métodos de entrega que se detallan a continuación.

Sectigo hace que todos sus certificados CA Root estén disponibles en el Repositorio.

Sectigo proporciona la cadena de certificados completa al suscriptor tras la emisión y entrega del certificado de suscriptor.

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 gestión de incidentes

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 establecidos para garantizar 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 adecuados de contingencia y recuperación ante desastres. Estos procedimientos definen y contienen un proceso formal 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 así como el procedimiento de comunicación a terceras partes. El proceso también permite analizar los incidentes de manera que se identifiquen las posibles causas, de modo que cualquier debilidad en los procesos de Sectigo pueda mejorarse para evitar que vuelva a ocurrir. Dichos planes se revisan y actualizan según sea necesario 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 incidente y el riesgo presentado a las partes afectadas. Dependiendo del alcance, Sectigo se reserva el derecho a revocar los certificados afectados, revocar claves, 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 clave privada de firma.

5.7.4. Procedimientos de compromiso de algoritmos

Los algoritmos criptográficos están expuestos a ataques y, por lo tanto, siguen siendo insuficientes para el uso previsto. Sectigo utiliza algoritmos adecuados que están actualizados. Sectigo no utiliza ningún algoritmo que no se considere adecuado para su uso de acuerdo con los diferentes estándares y mejores prácticas de la industria.

Para los suscriptores que solicitan certificados a Sectigo utilizando una CSR, Sectigo verifica el algoritmo utilizado por el suscriptor y rechaza la solicitud si este no está de acuerdo con los estándares.

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 una instalación de coubicación administrada por un centro de datos comercial, 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 fallo crítico 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, 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 y un sitio secundario en caso de que el sitio principal sufra una pérdida total de sistemas. Este plan de recuperación ante desastres establece que Sectigo se esforzará por minimizar las interrupciones en sus operaciones de CA.

5.8. Finalización del TSP

En caso de terminación de las operaciones como 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 de TSP, Sectigo tomará los siguientes pasos, cuando sea posible:

- Proporcionar a los Suscriptores de certificados válidos, Partes que Confían y otras partes afectadas con noventa (90) días de anticipación de su intención de dejar de actuar como TSP.
- Revocar todos los certificados que aún no estén 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 los arreglos razonables para preservar sus registros de acuerdo con esta DPC.
- 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.

En el caso de que Sectigo decida transferir la actividad a otro TSP, notificará al Órgano de Vigilancia y al suscriptor de sus certificados de los contratos de transferencia. A tal efecto, Sectigo remitirá el documento explicativo de las condiciones de transferencia así como las condiciones de uso que regularán las relaciones entre el suscriptor y el TSP al que se ceden los certificados.

El suscriptor debe dar su consentimiento expreso a la cesión de los certificados, aceptando las condiciones del TSP al que se ceden. Transcurrido el plazo de 90 días, sin contrato de transferencia o sin que el suscriptor lo acepte expresamente, los certificados serán revocados.

Cuando otro TSP con certificación cruzada de Sectigo detiene todas las operaciones, incluida la gestión de la revocación, todos los certificados cruzados a ese TSP se revocarán siguiendo las condiciones y requisitos establecidos anteriormente.

Estos requisitos pueden variar 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 del par de claves

6.1.1. Generación del par de claves

6.1.1.1. Pares de claves del suscriptor

Hay dos opciones para la generación del par de claves del suscriptor:

- Generado por el suscriptor
- Generado por Sectigo

En general, el suscriptor es el único responsable de la generación de un par de claves criptográficas asimétricas (RSA o ECDSA) apropiado para el tipo de certificado que se solicita. Durante la solicitud, el suscriptor generalmente deberá enviar una clave pública y otros detalles personales / corporativos en forma de solicitud de firma de certificado (CSR) o SPKAC.

Las solicitudes de QWAC generalmente se generan utilizando las funciones de generación de claves disponibles en el software del servidor web del Suscriptor.

Otras solicitudes generalmente se generan utilizando el software del módulo del proveedor de servicios criptográficos presente en los navegadores populares, aunque también pueden enviarse como PKCS # 10 o SPKAC.

Los certificados cualificados que proporcionen firmas cualificadas o sellos, respectivamente, se emitirán en QSCD. Los métodos aceptables para satisfacer este requisito incluyen (pero no se limitan a) los siguientes:

- Sectigo envía un módulo criptográfico de hardware adecuado, con un par de claves preinstaladas, en forma de tarjeta inteligente o dispositivo USB. Sectigo comprueba que el dispositivo sea un QSCD antes de usarlo y monitoriza su ciclo de vida:
    - Si un QSCD pierde su certificación antes de generar el par de claves y emitir un certificado, Sectigo reemplazará el QSCD con uno diferente aprobado, pero
    - Si un QSCD pierde su certificación mientras los certificados aún son válidos, Sectigo se comunicará con los clientes para reemplazar los certificados y tokens existentes por uno diferente que esté aprobado.
- El suscriptor contrafirma las solicitudes de certificado que se pueden verificar mediante el uso de un certificado del fabricante o una clave del fabricante que indique que la clave del suscriptor se administra en un módulo de hardware adecuado,
- El suscriptor proporciona una auditoría de TI adecuada que indica que su entorno operativo alcanza un nivel de seguridad al menos equivalente al de FIPS 140-2 nivel 3 o que figura como QSCD para certificados cualificados.

Cuando el suscriptor está generando, administrando y / o almacenando claves en un HSM en la nube (por ejemplo, Azure), el suscriptor debe proporcionar evidencia suficiente para demostrar que todos los pares de claves de la entidad final tienen:

a) ha sido generado

   1. utilizando un sistema confiable, tomando todas las precauciones razonables para evitar cualquier pérdida, divulgación o uso no autorizado de la clave privada, y luego transferida de forma segura a un HSM en la nube (por ejemplo, Azure); o

   2. generado directamente y almacenado en un HSM en la nube (por ejemplo, Azure).

b) almacenados en un HSM en la nube (por ejemplo, Azure).

6.1.1.2. Pares de claves de la CA y subCA

Para pares de claves de la CA raíz creados bajo esta DPC, Sectigo:

- prepara y sigue un guión de generación de claves,
- hace que un CAB sea testigo del proceso de generación del par de claves de la CA raíz o graba un video de todo el proceso de generación del par de claves de la CA raíz, y
- hace que un CAB emita un informe en el que se opina que la CA siguió su ceremonia de claves durante su proceso de generación de claves y certificados y los controles utilizados para garantizar la integridad y confidencialidad del par de claves.

Para otros pares de claves de la CA creados para Sectigo o un afiliado, Sectigo:

- prepara y sigue un guión de generación claves y
- hace que un CAB presencie el proceso de generación de pares de claves de la CA o graba un video de todo el proceso de generación de pares de claves de la CA

Las claves de la CA de Sectigo se generan en módulos de seguridad de hardware (HSM) que cumplen, como mínimo, con FIPS 140-2 nivel 3, están certificados de acuerdo con ISO / IEC 15408 o listados como QSCD. Las claves de la CA nunca están disponibles fuera del HSM en forma de texto sin formato. Todas las operaciones de generación de claves de la CA se realizan dentro de la seguridad del HSM, ya sea la generación de clave inicial o su uso final en el entorno de producción en vivo. Todas las claves que se exportan desde el HSM se cifran con un algoritmo de cifrado adecuado con la clave de cifrado generada por el HSM.

El acceso a las claves de la CA está restringido al personal autorizado y de confianza de Sectigo. Los datos clave de la CA deben almacenarse de forma segura en todo momento a menos que sea atendido por personal autorizado de Sectigo.

La generación de claves de la CA que involucra un HSM se realiza en una 'ceremonia de claves de la CA'. Todas las ceremonias de claves de la CA se realizan en un área segura y controlada. Durante la ceremonia, al menos dos miembros del personal autorizado de Sectigo están presentes en todo momento. Puede ser necesario que estén presentes auditores autorizados

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

Todas las ceremonias de claves de la CA se realizan en un ordenador con una instalación limpia verificada del sistema operativo que está aislado de todos los demás ordenadores en las diferentes redes. El software de control de operaciones criptográficas será una instalación nueva y se verificará que funcione correctamente antes de su uso.

Todos los medios creados a partir de una ceremonia de claves de la CA que contienen datos de respaldo de claves de la CA deben clasificarse y almacenarse de acuerdo con esta clasificación.

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

6.1.2. Entrega de la clave privada al suscriptor

Cuando las claves de suscriptor se generan en los servidores de Sectigo, se entregan al suscriptor a través de una comunicación cifrada.

Sectigo no genera claves para QWAC ni para otros certificados cualificados donde las claves se generan en el software del suscriptor.

Cuando Sectigo genera pares de claves para certificados cualificados, el personal autorizado de Sectigo entregará el dispositivo de módulo criptográfico certificado FIPS140-2, ISO 15408 o QSCD y un PIN imposible de adivinar al suscriptor nombrado en el certificado de suscriptor después de validar que su identidad coincide con el certificado de suscriptor. El dispositivo criptográfico se configurará para no permitir la exportación de la clave privada.

6.1.3. Entrega de la clave pública al emisor del certificado

Las solicitudes de QWAC se generan utilizando el software del servidor web del Suscriptor y la solicitud se envía a Sectigo en forma de una Solicitud de firma de certificado (CSR) PKCS # 10. La presentación se realiza electrónicamente a través del sitio web de Sectigo o mediante un RA aprobado por Sectigo.

Los certificados cualificados, no emitidos dentro de los dispositivos, aceptan las solicitudes generadas utilizando el software del proveedor de servicios criptográficos del suscriptor, se envían automáticamente a Sectigo en forma de una solicitud de firma de certificado (CSR) PKCS # 10. Se puede permitir que la clave privada permanezca en el proveedor de servicios criptográficos del suscriptor o se puede exportar al disco duro del suscriptor.

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

Las claves públicas de Sectigo se proporcionan a los terceros de confianza de varias formas. Una forma es a través del repositorio. Además, las claves públicas de las CA raíz de Sectigo están integradas en los navegadores.

6.1.5. Tamaños de clave

Los certificados raíz y cualquier certificado que se conecte a ellos tienen:

- Claves RSA cuyo tamaño en bits es divisible por 8 y es de al menos 2048 bits; o
- Claves ECDSA en las curvas P-256 o P-384.

6.1.6. Generación de parámetros de la clave pública

Las claves de CA de Sectigo se generan dentro de un HSM certificado por FIPS 140-2 Nivel 3 o ISO / IEC 15408.

Sectigo sigue las normas ETSI TS 119 312 y NIST SP 800-89 para RSA o NIST SP 800-56A para ECC.

6.1.7. Propósitos de uso de claves (según el campo de uso de claves X.509v3)

Los certificados cualificados de Sectigo son de uso general y pueden usarse sin restricción de área geográfica o industria. Para usar y confiar en un certificado cualificado de Sectigo, el tercero de confianza debe usar un software compatible con X.509v3. Los certificados cualificados de Sectigo incluyen campos de extensión de uso de claves para especificar los propósitos para los cuales se puede usar el certificado y para limitar técnicamente la funcionalidad del certificado cuando se usa con software compatible con X.509v3. La dependencia de los campos de extensión de uso clave depende de las implementaciones de software correctas del estándar X.509v3 y está fuera del control de Sectigo.

Los posibles propósitos identificados por el estándar X.509v3 son los siguientes:

1. Firma digital, para verificar firmas digitales, es decir, para autenticación de entidad y autenticación de origen de datos con integridad

2. No repudio, para verificar las firmas digitales utilizadas para proporcionar un servicio de no repudio que protege contra la entidad firmante que niega falsamente alguna acción.

3. Cifrado de claves, para cifrar claves u otra información de seguridad, p. Ej. Para el transporte de claves

4. Cifrado de datos, para cifrar datos de usuario, pero no claves u otra información de seguridad como en el punto anterior

5. Acuerdo de clave, para usar como clave de acuerdo de clave pública

6. Firma de certificado de clave, para verificar la firma de los certificados en una CA, utilizada solo en certificados de CA

7. Firma de CRL, para verificar la firma de una CA en las CRL

8. Solo cifrado, clave de acuerdo de clave pública para usar solo en el cifrado de datos cuando se usa con acuerdo de clave

9. Solo descifrar, clave de acuerdo de clave pública para usar solo para descifrar datos cuando se usa con acuerdo de clave

La aparición de un uso de clave en esta sección no indica que Sectigo emita o emitirá un certificado con ese uso de clave.

Las claves privadas correspondientes a los certificados raíz no se utilizarán para firmar certificados excepto en los siguientes casos:

1. Certificados autofirmados para representar a la propia CA raíz;

2. Certificados para CA subordinadas y certificados cruzados;

3. Certificados para fines de infraestructura (certificados de funciones administrativas, certificados de dispositivos operativos de CA internos); y

4. Certificados para verificación de respuesta OCSP.

6.2. Protección de la clave privada y controles del módulo criptográfico

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

6.2.1. Estándares y controles de módulos criptográficos

Sectigo genera y protege de forma segura su (s) propia (s) clave (s) privada (s), utilizando un sistema confiable y toma las precauciones necesarias para evitar el compromiso o el uso no autorizado de la misma. Dicho sistema deberá estar certificado al menos según FIPS 140-2 Nivel 3 o ISO / IEC 15408.

Las claves raíz de Sectigo se generan de acuerdo con las pautas detalladas en la Referencia de la ceremonia de generación de claves raíz. Las actividades realizadas y el personal involucrado en la Ceremonia de Generación de la Clave Raíz se registran para fines de auditoría. Las ceremonias posteriores de generación de claves raíz también deben seguir la guía de referencia documentada.

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

Todas las claves deben ser generadas por y en un módulo criptográfico. Las claves privadas se exportan desde el módulo criptográfico a tokens de respaldo solo para fines de transferencia de HSM, almacenamiento fuera de línea y respaldo. Las claves privadas se cifran cuando se transfieren fuera del módulo y nunca existen en forma de texto sin formato.

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 solo en formato cifrado.

Todas las transferencias de claves privadas hacia o desde un módulo criptográfico se realizan de acuerdo con los procedimientos especificados por el proveedor del módulo criptográfico correspondiente.

6.2.3. Almacenamiento de la clave privada en módulo criptográfico

Las claves privadas se generan y almacenan dentro de los módulos de seguridad de hardware (HSM) de Sectigo. Los HSM deben estar certificados con al menos FIPS 140-2 Nivel 3 o ISO / IEC 15408.

Para fines de recuperación de claves de la CA raíz, las claves de firma de la CA raíz se cifran y almacenan en un entorno seguro.

6.2.4. Método de activación de la clave privada

Según las circunstancias y el tipo de certificado, Sectigo, el suscriptor u otro personal autorizado pueden activar una clave privada. Las claves privadas de Sectigo se activan de acuerdo con las especificaciones del módulo criptográfico. El suscriptor debe hacer todos los esfuerzos razonables para proteger la integridad y confidencialidad de su (s) clave (s) privada (s). Las claves privadas permanecen activas hasta que se desactivan.

6.2.5. Método para desactivar la clave privada

Dependiendo de las circunstancias y el tipo de certificado, Sectigo, suscriptor u otro personal autorizado puede desactivar una clave privada.

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 puede comprender eliminarla del HSM o eliminarla del conjunto de respaldo activo. Las claves privadas se destruyen de acuerdo con la norma NIST SP 800-88.

6.2.7. Calificación del módulo criptográfico

Ver sección 6.2.1 de esta DPC.

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

Esta sección considera otras áreas de la gestión de las claves. Es posible que se apliquen subsecciones particulares a las CA emisoras, repositorios, CA, RA, Suscriptores y otros participantes.

6.3.1. Archivo de la clave pública

Cuando se archivan las claves públicas, se archivan de acuerdo con los procedimientos descritos en la sección 5.5 de esta DPC.

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

Los certificados son válidos tras su emisión por Sectigo y su aceptación por parte del suscriptor. Generalmente, el período de validez del certificado de suscriptor será de 1 a 3 años, sin embargo, Sectigo se reserva el derecho de ofrecer períodos de validez fuera de este período de validez estándar.

La duración de los certificados de CA subordinadas es igual o más corta que la de la CA por la que están firmadas.

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

Sectigo protege sus pares de claves de la CA Raiz de acuerdo con su infraestructura y su DPC. Los detalles del cumplimiento de Sectigo están disponibles en su sitio web oficial (*www.sectigo.com*).

Cuando un certificado de una CA está a punto de caducar, Sectigo genera un nuevo certificado de la CA con nuevas claves con tiempo de anticipación para cubrir el período de validez más largo de los certificados de entidad final emitidos por esa CA.

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 los datos de activación

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

6.4.2. Protección de los datos de activación

Los procedimientos utilizados para proteger los datos de activación dependen de si los datos son para tarjetas inteligentes o contraseñas. Las tarjetas inteligentes están en manos de personal de gran confianza. 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, como

- Aplicar los mismos controles de seguridad a todos los sistemas ubicados en la misma zona con un sistema certificado;
- 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;
- 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.

Los sistemas de CA imponen la autenticación de múltiples factores para todas las cuentas capaces de causar directamente la emisión del certificado.

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 PKI. 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 únicos 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 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 debe probar y aprobar 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.

Sectigo realiza auditorías internas trimestralmente para verificar y comprobar que todos los sistemas estén seguros y configurados correctamente.

6.7. Controles de seguridad de la red

Sectigo desarrolla, implementa y mantiene un programa de seguridad integral diseñado para proteger sus redes según las mejores prácticas de la industria (por ejemplo, los requerimientos del CABF reflejados en el documento Network and Certificate System Security Requirements). En este programa de seguridad, las protecciones generales para la red incluyen, entre otros:

- 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;
- Mantener los sistemas de la 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. Sello de tiempo

Sectigo opera una Autoridad de Sellado de Tiempo (TSA) cualificada.

Sectigo sincroniza todos los componentes de TSP con un servicio de hora proporcionado por varios servicios a través del servicio NTP (Network Time Protocol) en base a la hora proporcionada por laboratorios UTC(k). La hora derivada de este servicio horario se utiliza para establecer la hora de:

- Tipo de validez inicial de un certificado;
- Revocación de un certificado;
- Publicación de actualizaciones de CRL; y
- Respuestas OCSP.

La TSA cualificada de Sectigo está diseñada para usarse cuando sea necesario proporcionar el tiempo exacto para firmas o sellos y para brindar la integridad necesaria.

La TSA cualificada por Sectigo se encuentra en:

http://timestamp.sectigo.com/qualified

7. PERFILES DE CERTIFICADOS, CRL Y OCSP

Sectigo utiliza la versión 3 del estándar X.509 para construir certificados cualificados para su uso dentro de la PKI cualificada de Sectigo. X.509v3 permite que una CA agregue ciertas extensiones de certificado a la estructura básica del certificado. Sectigo utiliza una serie de extensiones de certificado para los fines previstos por X.509v3 según la Enmienda 1 de ISO / IEC 9594-8. X.509v3 es un estándar de la Unión Internacional de Telecomunicaciones para certificados digitales. Sectigo también utiliza diferentes estándares ETSI, como EN 319 412 parte 1 a 5 para extensiones adicionales y ETSI TS 119 495 para aquellos específicos de PSD2, la Directiva de servicios de pago.

7.1. Perfil del certificado

Sectigo incorpora por referencia la siguiente información en cada certificado cualificado que emite:

- Términos y condiciones.
- Cualquier otra política de certificado aplicable que se indique en un certificado Sectigo emitido, incluida la ubicación de esta DPC.
- Los elementos obligatorios del estándar X.509v3.
- Cualquier elemento no obligatorio pero personalizado del estándar X.509v3.
- Contenido de extensiones y nombres mejorados que no se expresan completamente en un certificado.
- Cualquier otra información que se indique en un campo de un certificado.

Un perfil de certificado contiene los campos que se especifican a continuación:

- campo de extensión de uso de claves (sección 6.1.7 de DPC)
- campo de criticidad de la extensión (sección 7.1.9 de la DPC)
- extensión de restricciones básicas (sección 7.1.7 de la DPC)

El contenido típico de la información publicada en un certificado de Sectigo puede incluir, entre otros, los siguientes elementos de información:

  - Nombre del solicitante o nombre de la organización.
  - Código del país del solicitante.
  - Nombre de la unidad organizativa, dirección postal, ciudad, estado.
  - Autoridad de certificación emisora (Sectigo).
  - Clave pública del solicitante.
  - Firma digital de Sectigo.
  - Algoritmo de firma.
  - Periodo de validez del certificado digital.
  - Número de serie del certificado digital.
  - qcStatements que indican las especificaciones de los certificados cualificados según lo establecido en los estándares de perfiles de certificados de ETSI.

- Los QWAC también tienen:
    - Nombre (s) de dominio completo del solicitante.

Sectigo genera números de serie de certificados no secuenciales mayores que cero (0) que contienen al menos 64 bits de salida de un CSPRNG.

7.1.1. Número (s) de versión

Todas las versiones del certificado son X.509 versión 3. El número de versión del certificado se establecerá en el valor entero de "2" para los certificados de la versión 3.

7.1.2. Extensiones del certificado

Las extensiones del certificado cumplen con la norma RFC 5280 como regla general.

Para los certificados cualificados, los estándares de ETSI requieren extensiones adicionales que deben cumplir los certificados de Sectigo.

La denominación mejorada es el uso de un campo de organización extendido en un certificado X.509v3. La información contenida en el campo de la unidad organizativa también se incluye en la extensión de la Política de certificados que Sectigo puede usar.

7.1.2.1. CA raíz

Los certificados de la CA Raiz de Sectigo contienen:

- una extensión basicConstraints marcada como crítica. El campo cA se establece como verdadero. PathLenConstraint no está presente.
- una extensión keyUsage marcada como crítica. Se establecen las posiciones de bit para keyCertSign, digitalSignature y cRLSign.

Los certificados de la CA Raiz de Sectigo pueden contener una extensión cRLDistributionPoints no crítica que contiene la URL HTTP del servicio CRL de la CA.

Los certificados de la CA Raiz de Sectigo no contienen una extensión certificatePolicies ni la extensión de claves de uso extendidas.

7.1.2.2. CA subordinadas

Los certificados de CA subordinada de Sectigo contienen:

- una extensión cRLDistributionPoints no crítica que contiene la URL HTTP del servicio CRL de la CA emisora.
- una extensión AuthorityInformationAccess no crítica que contiene la URL HTTP del respondedor OCSP de la CA emisora y que contiene la URL HTTP del certificado de la CA emisora.

- una extensión basicConstraints marcada como crítica. El campo cA se establece como verdadero. El pathLenConstraint a menudo está presente y pathLenConstraint generalmente se establece en 0.
- una extensión keyUsage marcada como crítica. Se establecen las posiciones de bit para keyCertSign, digitalSignature y cRLSign.
- Una extensión ExtendedKeyUsage marcada como no crítica.

7.1.2.3. Certificados de suscriptor

Los certificados de suscriptor de Sectigo contienen:

- una extensión de certificatePolicies que incluye uno o más policyIdentifiers y generalmente contiene un policyQualifier que hace referencia al URI de la DPC pero no incluye un userNotice.
- una extensión AuthorityInformationAccess no crítica que contiene la URL HTTP del respondedor OCSP de la CA emisora y que contiene la URL HTTP del certificado de la CA emisora.
- una extensión basicConstraints marcada como crítica. El campo cA no está configurado.
- una extensión keyUsage marcada como crítica. Las posiciones de bit para keyCertSign y cRLSign NO se establecen.

Los certificados de suscriptor de Sectigo pueden contener una extensión cRLDistributionPoints no crítica que contiene la URL HTTP del servicio CRL de la CA emisora.

Para obtener información adicional, consulte el documento de perfiles de certificado.

7.1.2.4. Todos los certificados

Todos los demás campos y extensiones están de acuerdo con RFC5280 y ETSI EN 319 412 parte 1 a 5 y ETSI TS 119 495 específicamente para certificados PSD2.

Sectigo no emite certificados que contengan valores de keyUsage o extendedKeyUsage, o extensiones de certificado, u otros datos no especificados en las secciones 7.1.2.1, 7.1.2.2 o 7.1.2.3 anteriores, a menos que Sectigo tenga conocimiento de una razón para incluir los datos en el certificado.

Sectigo no emite certificados que contengan extensiones a menos que:

- dicho valor cae dentro de un arco de OID para el cual el solicitante demuestra propiedad, o
- el solicitante puede demostrar de otro modo el derecho a hacer valer los datos en un contexto público

Sectigo no emite certificados que contengan semántica que, si se incluyen, inducirán a error al tercero de confianza sobre la información del certificado verificada por Sectigo.

7.1.2.5. Aplicación de RFC 5280

Solo para QWAC, así como para todos los demás tipos de certificados SSL / TLS, y para fines de aclaración, un precertificado, como se describe en RFC 6962 - Transparencia del certificado, no se considerará un "certificado" sujeto a los requisitos de RFC 5280 - Certificado de infraestructura de clave pública X.509 de Internet y perfil de lista de revocación de certificados (CRL) según esta DPC.

7.1.3. Identificadores de objetos de algoritmo

Los certificados de Sectigo se firman mediante algoritmos que incluyen, entre otros, RSA y ECDSA.

Los certificados de Sectigo se firman mediante algoritmos con algunos de estos identificadores:

sha-1WithRSAEncryption	OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)pkcs-1(1) 5 }
sha256WithRSAEncryption	OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }
sha384WithRSAEncryption	OBJECT IDENTIFIER ::= { iso(1)member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }
ecdsa-with-SHA256	OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }
ecdsa-with-SHA384	OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }

Sectigo no firma certificados utilizando RSA con PSS. Los certificados de CA, los certificados calificados de suscriptor y los certificados OCSP no están firmados con sha-1WithRSAEncryption.

Para ECDSA, Sectigo usa y acepta solo las curvas NIST Suite B para aquellas claves enviadas a Sectigo para su inclusión en los certificados de entidad final.

7.1.4. Formas de nombres

Las formas de nombres son los estipulados en 3.1.1 de esta DPC.

7.1.4.1. Codificación

El contenido del campo Nombre distinguido del emisor del certificado coincide con el DN del sujeto de la CA emisora para admitir el encadenamiento de nombres como se especifica en RFC 5280, sección 4.1.2.4.

7.1.4.2. Información del asunto: certificados de suscriptor

Sectigo declara que sigue el procedimiento establecido en esta DPC para verificar que, a la fecha de emisión del certificado, toda la información del sujeto es precisa.

Para obtener información adicional, consulte el documento de perfiles de certificado.

7.1.4.3. Información del asunto: certificados raíz y certificados de CA subordinada

Sectigo declara que sigue el procedimiento establecido en su Política de certificados y / o Declaración de prácticas de certificación para verificar que, a la fecha de emisión del certificado, toda la información del Sujeto es precisa.

7.1.4.3.1. Campos de nombre distinguido del sujeto

1. nombre común

   Este campo estará presente y se puede utilizar como identificador para el certificado de CA. En todos los certificados de CA emitidos por Sectigo, cada sujeto único: commonName se emparejará con un solo par de claves de CA.

2. Nombre de la Organización

   Este campo estará presente y contendrá el nombre de la CA del sujeto o DBA como se verifica en la Sección 3.2.

   Sectigo puede incluir información en este campo que difiera ligeramente del nombre verificado, como variaciones o abreviaturas comunes, siempre que las abreviaturas utilizadas sean abreviaturas aceptadas localmente; por ejemplo, si el registro oficial muestra "Nombre de la empresa incorporado", Sectigo puede utilizar "Nombre de la empresa Inc." o "Nombre de la empresa".

3. nombre del país

   Este campo estará presente y contendrá la información del código de país ISO 3166-1 de dos letras del Sujeto, como se verifica en la sección 3.2.

7.1.5. Restricciones de nombres

Sectigo incluye restricciones de nombres en los certificados de la sCA subordinada cuando sea relevante. Sectigo coloca las restricciones de nombres en una extensión no crítica dentro del certificado de la CA.

Sectigo no incluye el EKU anyExtendedKeyUsage en los certificados de CA con restricción de nombre.

7.1.6. Identificador de objeto de política de certificado

Sectigo usa políticas OID bajo los arcos:

iso (1) organización identificada (3) dod (6) internet (1) privada (4) empresa (1)
6449
certificados (1) políticas (2),

y:

joint-iso-itu-t (2) organizaciones-internacionales (23) ca-browser-forum (140) políticas-de-certificados (1)

y:

itu-t (0)
organización identificada (4)
etsi (0)
id-cert-profile (194112)
identificadores de políticas (1)
qcp-natural (0), qcp-legal (1), qcp-natural-qscd (2), qcp-legal-qscd (3), qcp-web (4)

Consulte el Anexo B para obtener información adicional.

7.1.7. Sintaxis y semántica de las políticas

Sectigo incluye en los certificados de entidad final una extensión de política de certificado no crítica como se define en RFC5280. Sectigo incluye una extensión de PolicyInformation única que incluye el Identificador de política de certificado y un Cualificador de política único que hace referencia a este URI de DPC, pero sin incluir un UserNotice.

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 a los terceros de confianza que consulten los directorios de certificados y precertificados revocados en todo momento antes de confiar en la información incluida en un certificado. La CRL para cualquier certificado emitido por Sectigo (ya sea certificado de suscriptor o certificado de CA) se puede encontrar en la URL codificada dentro del campo CRLDP del propio certificado.

El perfil de la CRL de Sectigo es:

Versión	[Valor 1]	
Nombre del emisor	CountryName = [Nombre del país del certificado raíz], OrganizationName = [Organización del certificado raíz], CommonName = [Nombre común del certificado raíz] [Codificación UTF8String]	
Esta actualización	[Fecha de emisión]	
Próxima actualización	[Fecha de emisión + no más de 10 días]	
	Entradas de CRL	

Certificados revocados	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

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

Si está presente, la extensión de código de motivo no se marcará como crítica y no estará sin especificar (0). Si la entrada de CRL es para un certificado de CA raíz o CA subordinada, la extensión de código de motivo estará presente.

Si no se especifica el motivo de la revocación, se omite la extensión del código de motivo.

Si está presente una extensión de entrada de ReasonCode en la CRL, esta razón indica el motivo más apropiado para la revocación del certificado (elegido por el suscriptor en el caso de los Certificados QWAC al crear la solicitud de revocación), como se define a continuación:

- cessationOfOperation: este motivo se utiliza cuando el suscriptor ya no controla o no está autorizado para usar los nombres de dominio, o el suscriptor no está usando el certificado o Sectigo tiene conocimiento de alguna circunstancia en la que el certificado ya no está permitido

- keyCompromise: este motivo se utiliza cuando Sectigo ha recibido pruebas o sospechas razonables de que la clave privada está comprometida

- caCompromise: este motivo se usa cuando Sectigo ha recibido pruebas o sospechas razonables de que la clave de la CA está comprometida

- privilegeWithdrawn: este motivo se usa cuando hay una infracción del lado del suscriptor que no ha resultado en un problema de clave comprometida, por ejemplo, información engañosa o incorrecta en el certificado.

- afiliationChanged: este motivo se utiliza cuando el nombre del sujeto u otra información de la identidad del sujeto en el certificado ha cambiado

- superseded: este motivo se usa cuando el suscriptor ha solicitado un reemplazo o Sectigo ha obtenido información de que la información validada del dominio no es confiable o no cumple con este documento o con los requisitos del CAB Forum

La extensión de CRL “ExpiredCertsOnCRL” está incluida en todas las CRL bajo la jerarquía eIDAS de Sectigo según lo definido por ISO / IEC 9594-8.

Sectigo hace una comprobación byte por byte del nombre del emisor entre los certificados de CA y las CRL.

7.3. Perfil OCSP

Sectigo también 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 y precertificados emitidos bajo los términos de esta DPC. Si se le solicita un certificado que no haya sido emitido por Sectigo, el respondedor proporcionará 'no autorizado'.

Para los certificados cualificados, los respondedores OCSP continuarán dando un estado "bueno" a los certificados no revocados incluso después de su vencimiento.

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.

El perfil de las respuestas de Sectigo OCSP es según esta tabla:

Extensión		**Valor**
Estado de respuesta OCSP		exito (0x0)
Tipo de respuesta		Respuesta OCSP básica
Versión		1 (0x0)
ID del respondedor		Igual que el identificador de la clave del sujeto que aparece en el certificado de firma.
Producido en		[el momento en que se firmó esta respuesta]
Respuestas		
Certificado	IDENTIFICACIÓN	
	Algoritmo hash	Sha1
	Hash del nombre del emisor	Hash del DN del emisor
	Hash de clave de emisor	Hash de la clave pública del emisor
	Número de serie	CertificateSerialNumber
Estado del certificado		Bueno / revocado / desconocido
Tiempo de revocación (si se revocó)		[El momento en el que el certificado fue revocado o puesto en espera]
Esta actualización		[La hora más reciente en la que el respondedor sabe que el estado del certificado indicado es correcto]
Próxima actualización		[La hora a la que estará disponible información más reciente sobre el estado del certificado o antes].
Algoritmo de firma		sha256WithRSAEncryption

Si una respuesta OCSP es para un certificado de CA raíz o CA subordinada, incluidos los certificados cruzados, y ese certificado ha sido revocado, entonces el campo revocationReason dentro de RevokedInfo del CertStatus estará presente.

El CRLReason indicado contiene un valor permitido para las CRL, como se especifica en la Sección 7.2.2.

El respondedor OCSP para nuestra jerarquía eIDAS utiliza la extensión ArchiveCutOff como se especifica en RFC 6960 con la fecha ArchiveCutOff establecida en el valor de fecha y hora del certificado “notBefore” de la CA.

7.3.1. Número (s) de versión

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

8. AUDITORÍA DE CUMPLIMIENTO Y OTRAS EVALUACIONES

Las prácticas especificadas en esta DPC han sido diseñadas para cumplir o superar los requisitos de los estándares de la industria 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 evalúa el cumplimiento de Sectigo con eIDAS y ETSI realizando una auditoría periódica.

8.1. Frecuencia o circunstancias de la evaluación

El esquema de 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 con una auditoría de seguimiento anual.

8.2. Identidad / Cualificaciones del evaluador

Para las auditorías ETSI / eIDAS, estas deberán ser realizadas por un CAB certificado o acreditado.

En cualquier caso, un CAB significa un (grupo de) personas físicas o jurídicas que colectivamente poseen las siguientes calificaciones y habilidades:

1. Independencia del tema de la auditoría;
2. La capacidad de realizar una auditoría que aborde los criterios especificados en un esquema de auditoría elegible (consulte la Sección 8.1);
3. 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;
4. Estar acreditado según ETSI EN 319 403 y/o ISO 17065;
5. Obligado por la ley, la regulación gubernamental o el código de ética profesional

8.3. Relación del evaluador con la entidad evaluada

El CAB es independiente de Sectigo y no tiene ningún interés financiero, relación comercial o curso de 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 evaluación

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

- Divulgación de prácticas comerciales

    - la CA divulga sus prácticas comerciales, y
    - la CA presta sus servicios de acuerdo con su DPC
- Gestión del ciclo de vida de la clave
    - la CA mantiene controles efectivos para proporcionar una seguridad razonable de que la integridad de las claves y los certificados que administra está establecida y protegida durante sus ciclos de vida.
- Gestión del ciclo de vida del certificado
    - La CA mantiene controles efectivos para proporcionar una seguridad razonable de que la información del Suscriptor se autenticó adecuadamente para actividades de registro específicas, y
    - La CA mantiene controles efectivos para proporcionar una garantía razonable de que las solicitudes de certificado de la CA subordinada son precisas, autenticadas y aprobadas.
- Control de la CA
    - la CA mantiene controles efectivos para proporcionar una seguridad razonable de que
        - El acceso lógico y físico a los sistemas y datos de la 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 la CA están debidamente autorizados y realizados para mantener la integridad de los sistemas de la CA.

Se pueden consultar los estándares ETSI en *https://www.etsi.org* o en el Anexo D.

8.5. Acciones a realizar como resultado de una deficiencia

El auditor 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

Esta parte describe las representaciones legales, garantías y limitaciones asociadas con los certificados digitales de Sectigo.

9.1. Tarifa

Sectigo puede cobrar tarifas de Suscriptor por algunos o todos los servicios de certificados que Sectigo ofrece, incluida la emisión, renovación y reemisiones (de acuerdo con la Política de reemisión de Sectigo establecida en 9.1.6 de esta DPC). Dichas tarifas se detallan en el sitio web de Sectigo o en el acuerdo de suscripción aplicable.

Sectigo se reserva el derecho a modificar dichas tarifas. Se informará adecuadamente a los distribuidores y revendedores de Sectigo sobre las modificaciones de precios según se detalla en los acuerdos de socios relevantes.

9.1.1. Tarifas de emisión o renovación de certificados

Sectigo puede 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 del Suscriptor o en el sitio web de Sectigo.

9.1.2. Tarifas de acceso al certificado

Sectigo 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 u OCSP.

9.1.4. Politica de reembolso

Sectigo ofrece una política de reembolso de 30 días. Durante el período de 30 días, comenzando cuando se emite un certificado por primera vez, el suscriptor puede solicitar un reembolso completo por su certificado. En tales circunstancias, el certificado original puede ser revocado y se puede proporcionar un reembolso al suscriptor. Sectigo no está obligado a reembolsar un certificado después de que haya expirado el período de 30 días.

9.1.5. Política de reemisión

Sectigo ofrece una política de reemisión de 30 días. Durante el período de 30 días, a partir de la primera emisión de un certificado, el suscriptor puede solicitar una nueva emisión de su certificado y no incurrir en cargos adicionales por la reemisión. Si otros detalles además de la clave pública requieren enmiendas, Sectigo se reserva el derecho de revalidar la aplicación de acuerdo con los procesos de validación detallados en esta DPC. Si la solicitud de reemisión no pasa el proceso de validación, Sectigo se reserva el derecho de rechazar la solicitud de

reemisión. En tales circunstancias, el certificado original puede ser revocado y se puede proporcionar un reembolso al suscriptor.

Sectigo no está obligado a volver a emitir un certificado una vez transcurrido el período de 30 días.

9.2. Responsabilidad financiera

9.2.1. Cobertura del seguro

Sectigo mantiene un seguro profesional de errores y omisiones.

9.2.2. Cobertura de seguro o garantía para entidades finales

Si Sectigo fue negligente al emitir un certificado que resultó en una pérdida para un tercero de confianza, el tercero de confianza puede ser elegible bajo la Garantía del tercero de confianza de Sectigo para recibir hasta la Cobertura Máxima del Certificado por Incidente, sujeto al Límite de Pago Total, para todas las reclamaciones relacionadas con ese certificado. Para conocer los términos y condiciones completos, consulte el Acuerdo del tercero de confianza y la Garantía del tercero de confianza en el Repositorio.

9.3. Confidencialidad de la información comercial

Sectigo observa las reglas aplicables sobre la protección de datos personales según lo considere la ley o la política de privacidad de Sectigo (consulte la sección 9.4.1 de esta DPC) como 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 que no es de confianza:

- 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.
- 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 o el formulario de solicitud de certificado que se envía como parte de una solicitud de certificado se publican dentro de un certificado emitido. Dicha información no está dentro del alcance de la información confidencial.

9.3.3. Responsabilidad de proteger la información confidencial

El personal de Sectigo en puestos de confianza maneja la información confidencial con estricta confidencialidad y debe firmar acuerdos de confidencialidad antes de ser empleado en un puesto de confianza.

El personal de Sectigo, especialmente aquellos en la RA / LRA, debe cumplir con los requisitos de las leyes de protección de datos aplicables, es decir, GDPR, sobre la protección de información confidencial.

9.3.4. Publicación de datos de revocación de certificados

Sectigo se reserva el derecho de publicar una CRL según se indique.

9.4. Privacidad de la información personal

9.4.1. Plan de privacidad

Sectigo ha implementado una Política de Privacidad, que cumple con esta DPC. La Política de privacidad se publica en *https://sectigo.com/privacy-policy* (ver cláusula 1.6.2).

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 confidencial 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 confidencial.

9.4.4. Responsabilidad de proteger la información confidencial

Se espera que los participantes de Sectigo manejen la información confidencial con cuidado y de conformidad con las leyes de privacidad locales de la jurisdicción correspondiente.

9.4.5. Aviso y consentimiento para usar información confidencial

Sectigo solo utilizará información confidencial de acuerdo con la Política de privacidad.

9.4.6. Divulgación de conformidad con un proceso judicial o administrativo

Sectigo se reserva el derecho de divulgar información personal si Sectigo cree razonablemente que

- la divulgación es requerida por ley o reglamento, o
- la divulgación es necesaria en respuesta a un proceso judicial, administrativo u otro proceso legal.

9.4.7. Otras circunstancias de divulgación de información

Consulte la Política de privacidad. Además, Sectigo no está obligado a divulgar ninguna información personal, a menos que la ley exija lo contrario, sin una solicitud autenticada y razonablemente específica de una parte autorizada que especifique:

- La parte a la que Sectigo tiene el deber de mantener la confidencialidad de la información;
- La parte que solicita dicha información; y
- Una orden judicial, si la hubiera.

9.5. Derechos de propiedad intelectual

Sectigo o sus socios o asociados poseen todos los derechos de propiedad intelectual asociados con sus bases de datos, sitios web, certificados digitales de Sectigo y cualquier otra publicación originada en Sectigo, incluida esta DPC.

9.6. Representaciones y garantías

9.6.1. Representaciones y garantías de la CA

Sectigo hace ciertas representaciones con respecto a su servicio público a todos los Suscriptores y partes de confianza, como se describe a continuación. Sectigo se reserva el derecho de modificar tales representaciones como lo considere oportuno o según lo requiera la ley.

Salvo que se indique expresamente en esta DPC o en un acuerdo separado con el Suscriptor, en la medida especificada en las secciones relevantes de esta DPC, Sectigo representa, en todos los aspectos materiales, a:

- Cumplir con esta DPC 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), violación de datos o cualquier otro incidente de seguridad relacionado con los datos privados de los suscriptores y terceros de confianza.
- Proporcionar y validar los procedimientos de solicitud para los distintos tipos de certificados que puede poner a disposición del público.
- Emitir certificados de acuerdo con esta DPC y cumplir con sus obligaciones aquí presentadas.
- Al recibir una solicitud de una RA que opera dentro de la red de Sectigo, actuar con prontitud para emitir un certificado de acuerdo con esta DPC.
- Al recibir una solicitud de revocación de una RA que opera dentro de la red de Sectigo, actuar con prontitud para revocar un certificado de acuerdo con esta DPC.
- Publicar los certificados aceptados de acuerdo con esta DPC.
- Brindar soporte a los suscriptores y partes de confianza como se describe en esta DPC.
- Revocar certificados de acuerdo con esta DPC.
- Prever la caducidad y renovación de certificados de acuerdo con esta DPC.
- Ponga a disposición de las partes solicitantes una copia de esta DPC y las políticas aplicables.

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 del seguro de Sectigo y de acuerdo con esta DPC.

El Suscriptor también reconoce que Sectigo no tiene más obligaciones en virtud de esta DPC.

9.6.2. Representaciones y garantías de la RA

La RA de Sectigo opera bajo las políticas y prácticas detalladas en esta DPC y también los acuerdos asociados de revendedor y revendedor de alojamiento web. La RA está obligada por contrato a:

- Recibir solicitudes de certificados Sectigo de acuerdo con esta DPC.
- Realizar todas las acciones de verificación prescritas por los procedimientos de validación de Sectigo y esta DPC.
- 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.
- Cumplir con todas las leyes, normas y reglamentos aplicables al desempeño de sus funciones como RA.

9.6.3. Declaraciones y garantías de los suscriptores

Los suscriptores declaran y garantizan que cuando se envían a Sectigo no interfieren ni infringen ningún derecho de terceros en ninguna jurisdicción con respecto a sus marcas

comerciales, marcas de servicio, nombres comerciales, nombres de empresas o cualquier otro derecho de propiedad intelectual, y que no pretenden utilizar la información para ningún fin ilícito, que incluye, entre otros, interferencia ilícita con el contrato o una ventaja comercial potencial, competencia desleal, dañar la reputación de otra persona y confundir o engañar a cualquier persona física o jurídica.

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:

- Las firmas digitales creadas utilizando la Clave Privada correspondiente a la Clave Pública incluida en el certificado es la firma digital del Suscriptor y el certificado ha sido aceptado y está debidamente operativo en el momento en que se crea la firma digital.
- Ninguna persona no autorizada ha tenido acceso a la clave privada del suscriptor.
- Todas las declaraciones hechas por el suscriptor de Sectigo con respecto a la información contenida en el certificado son precisas y verdaderas.
- Toda la información contenida en el certificado es precisa y verdadera según el mejor conocimiento del suscriptor o en la medida en que el Suscriptor haya recibido un aviso de dicha información, mientras que el Suscriptor actuará de inmediato para notificar a Sectigo de cualquier inexactitud material en dicha información.
- El certificado se utiliza exclusivamente para fines legales y autorizados, y de conformidad con esta DPC.
- El suscriptor retiene el control de su clave privada, usa un sistema confiable y toma 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.
- El suscriptor acepta los términos y condiciones de esta DPC y otros acuerdos y declaraciones de política de Sectigo.
- El suscriptor cumple con las leyes y regulaciones aplicables en las jurisdicciones en las que opera, incluidas las relacionadas con la protección de la propiedad intelectual, virus, acceso a sistemas informáticos, etc.
- El suscriptor cumple con todas las leyes y regulaciones de exportación para productos de doble uso, según corresponda.

En todos los casos y para 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 sobre dichos cambios.

9.6.4. Declaraciones y garantías de los terceros de confianza

Una parte que confía acepta que para poder confiar razonablemente en un certificado cualificado de Sectigo, el tercero de confianza debe:

- Minimizar el riesgo de depender de una firma digital creada por un certificado inválido, revocado, vencido o rechazado;
- Haber realizado esfuerzos razonables para adquirir conocimientos suficientes sobre el uso de certificados cualificados y PKI.
- Leer y aceptar los términos del contrato según la DPC de Sectigo y el tercero de confianza.
- Verificar un certificado cualificado 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 OCSP de Sectigo.
- Confiar en un certificado cualificado de Sectigo solo si es válido y no ha sido revocado o vencido.
- Confiar en un certificado cualificado de Sectigo, solo cuando sea razonable en las circunstancias enumeradas en esta sección y otras secciones relevantes de esta DPC.

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 exactitud, 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 relevante a continuación en esta DPC y en la póliza de seguro de Sectigo.
- Representaciones hechas con respecto a la información contenida en un certificado, excepto cuando se indique en la descripción del producto relevante en esta DPC.
- La calidad, funciones o rendimiento de cualquier dispositivo de software o hardware.
- La revocación de un certificado, si Sectigo no puede revocar el certificado por motivos ajenos 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 esta DPC. Sectigo no declara ni garantiza que dicho software de usuario admitirá y hará cumplir los controles requeridos por Sectigo, mientras que el usuario debe buscar el asesoramiento adecuado.

9.8. Limitaciones de responsabilidad

Sectigo cumple con el artículo 13 del reglamento eIDAS.

Los certificados pueden incluir una breve declaración que describa 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 puedan aplicarse. Los suscriptores deben aceptar los Términos y condiciones de Sectigo antes de registrarse para obtener un certificado. Para comunicar esta información, Sectigo puede utilizar:

- Un atributo de unidad organizativa.
- Un cualificador 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 en el caso de fraude o mala conducta intencionada de Sectigo) será la responsabilidad total de Sectigo para con todas las partes, incluidos, entre otros, un Suscriptor, un solicitante, un destinatario o un tercero de confianza para todas las firmas digitales y transacciones relacionadas con dicho certificado exceder la responsabilidad máxima acumulativa para dicho certificado según se establece en el seguro de Sectigo.

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 o consecuente.
- 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 digitales.
- Cualquier otra transacción o servicio ofrecido en el marco de esta DPC.
- Cualquier otro daño, excepto los debidos a la confianza en la información verificada en un certificado.
- Cualquier responsabilidad debido a fraude o mala conducta intencional del solicitante, incluida la provisión por parte del solicitante de información falsa o engañosa durante el proceso de verificación de un certificado.
- Cualquier responsabilidad que surja del uso de un certificado que no haya sido emitido o usado de acuerdo con esta DPC.

- 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 establecidas en él o en esta DPC.
- Cualquier responsabilidad que surja de la seguridad, la usabilidad, la 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 Sectigo

En la medida en que lo permita la ley aplicable, Sectigo indemnizará a cada Proveedor de software de aplicación contra cualquier reclamación, daño o pérdida de terceros que sufra un Proveedor de software de aplicación en relación con un Certificado emitido por Sectigo que no cumpla con la regulación eIDAS o cualquier otro estándar de la industria vigente a la fecha de emisión del Certificado, independientemente de la causa de la acción o la teoría legal involucrada, excepto cuando el reclamo, daño o pérdida sufrida por el Proveedor de software de aplicación fue causado directamente por el software del Proveedor de software de aplicación que muestra ya sea (1) un Certificado válido y confiable como no válido o confiable o (2) mostrando como confiable (i) un Certificado que ha caducado o (ii) un Certificado revocado donde el estado de revocación está disponible en línea pero el software del Proveedor de software de aplicación no pudo verificar o ignorar el estado.

9.9.2. 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 honorarios razonables 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 fallo 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.
- Violación de cualquier ley o reglamento aplicable, ya sea local o extranjero, incluidos, entre otros, los relacionados con la protección de la propiedad intelectual, virus, acceso a sistemas informáticos, protección de datos y cumplimiento de exportaciones.

- Infracción de los derechos de propiedad intelectual de un tercero.

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.

9.9.3. Indemnización por parte de las partes que confían

En la medida en que lo permita la ley, cada Parte que Confía deberá indemnizar a Sectigo, sus socios y cualquier entidad con firma cruzada, y sus respectivos directores, funcionarios, empleados, agentes y contratistas por cualquier pérdida, daño o gasto, incluidos los honorarios razonables de abogados, relacionado con (i) el incumplimiento del Acuerdo de la Parte que Confía, un Acuerdo de Licencia de Usuario Final, esta DPC o la ley aplicable por parte de la Parte que Confía; (ii) confianza irrazonable en un Certificado; o (iii) no verificar el estado del Certificado antes de su uso.

9.10. Duración y Terminación

9.10.1. Término

El término de esta DPC, incluidas las enmiendas y adiciones, comienza con la publicación en el Repositorio y permanece en vigor hasta que se reemplaza por una nueva DPC aprobada por la Autoridad de Políticas de Sectigo.

9.10.2. Terminación

Esta DPC, incluidas todas las enmiendas y adiciones, permanecerá en vigor hasta que sea reemplazada por una versión más nueva.

9.10.3. Efecto de terminación y supervivencia

Los siguientes derechos, responsabilidades y obligaciones sobreviven a la terminación de esta DPC para los certificados emitidos en virtud de esta DPC:

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

Tras la terminación de esta DPC, todos los participantes de PKI están sujetos a los términos de esta DPC para los certificados emitidos durante la vigencia de esta DPC 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 esta DPC 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, edificio 26 Exchange Quay, Trafford Road
Salford, Greater Manchester, M5 3EQ, Reino Unido
Correo electrónico: *legalnotices@sectigo.com*

Esta DPC, los acuerdos relacionados y las políticas de certificados a las que se hace referencia en este documento están disponibles en línea en el Repositorio.

9.12. Enmiendas

Tras un cambio material en esta DPC, se publicará una edición actualizada de esta DPC en el repositorio de Sectigo (disponible en *https://www.sectigo.com/legal*), con una numeración de versión incremental adecuada que se utiliza para identificar nuevas ediciones. Esta DPC se actualiza al menos una vez al año.

Existen controles para garantizar razonablemente que la DPC de Sectigo no se modifica ni se publica sin la autorización previa de la Autoridad de Políticas de Sectigo.

9.12.1. Procedimiento de modificación

Cuando la Autoridad de Políticas de Sectigo haga una enmienda a esta DPC, aprobará dichas enmiendas y Sectigo las publicará en el Repositorio. Las enmiendas pueden ser una actualización, revisión o modificación de este documento de la DPC y se pueden detallar en esta DPC o en un documento separado. Además, las enmiendas reemplazan cualquier disposición designada o en conflicto de la versión enmendada de esta DPC.

9.12.2. Mecanismo y período de notificación

Sectigo puede notificar una enmienda a esta DPC publicándola 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 DPC, 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 a esta DPC 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

Esta DPC se rige e interpreta de acuerdo con el reglamento eIDAS, para garantizar una interpretación uniforme de esta DPC, independientemente del lugar de residencia o lugar de uso de los productos y servicios cualificados por Sectigo. La regulación eIDAS se aplica a todas las relaciones comerciales o contractuales de Sectigo en las que esta DPC puede aplicarse o citarse implícita o explícitamente en relación con los productos y servicios cualificados de Sectigo en los que Sectigo actúa como proveedor.

9.14.2. Interpretación

Esta DPC 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 certificado. Al interpretar esta DPC, 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 de esta DPC están pensados únicamente para su conveniencia y referencia y no deben utilizarse para interpretar, interpretar o hacer cumplir cualquiera de las disposiciones de esta DPC.

Los apéndices y definiciones de esta DPC son, a todos los efectos, una parte integral y vinculante de esta DPC.

9.14.3. Jurisdicción

Cada parte, incluidos los socios de Sectigo, los suscriptores y los terceros de confianza, acuerda irrevocablemente que los tribunales de Barcelona en España tienen jurisdicción exclusiva para conocer y decidir cualquier demanda, acción o procedimiento, y resolver cualquier disputa que pueda surgir de o en conexión con esta DPC.

9.15. Cumplimiento de la ley aplicable

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

9.16. Otras disposiciones

9.16.1. Acuerdo completo

Esta DPC 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.

9.16.2. Asignación

Esta DPC será vinculante para los sucesores, albaceas, herederos, representantes, administradores y cesionarios, ya sean expresos, implícitos o aparentes, de las partes. Los derechos y obligaciones detallados en esta DPC son asignables por las partes, por aplicación de la ley (incluso como resultado de una fusión o transferencia de una participación mayoritaria en valores con derecho a voto) o de otro modo, siempre que dicha asignación se realice de conformidad con los artículos de esta DPC sobre terminación o cese de operaciones, y siempre que dicha cesión no produzca una novación de cualquier otra deuda u obligación que la parte cedente tenga con otras partes en el momento de dicha cesión.

9.16.3. Divisibilidad

Si algún término, disposición, pacto o restricción contenida en esta DPC, o la aplicación de la misma, por cualquier motivo y en cualquier medida se considera inválido, nulo o inaplicable, (i) dicha disposición se reformará en la medida mínima. necesario para hacerla válida y exigible que afecte la intención original de las partes, y (ii) el resto de los términos, disposiciones, convenios y restricciones de esta DPC permanecerán en pleno vigor y efecto y de ninguna manera se verán afectados, deteriorado o invalidado.

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

Esta DPC se aplicará en su totalidad, mientras que el incumplimiento por parte de cualquier persona de cualquier disposición de esta DPC 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 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 la DPC de Sectigo, cualquier Acuerdo de suscripción o cualquier Acuerdo de parte que confía debido a cualquier causa fuera de su control razonable, que, a modo de ejemplo, incluye casos fortuitos o del enemigo público, disturbios e insurrecciones, guerras, accidentes, incendios, huelgas y otras dificultades laborales (esté o no Sectigo en un posición para ceder a tales demandas), embargos, acciones judiciales, fallo 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 esta DPC entre en conflicto con otras reglas, pautas o contratos, esta DPC prevalecerá y vinculará al Suscriptor y a otras partes, excepto en lo que respecta a otros contratos:

- Antes del primer lanzamiento público de la versión actual de esta DPC.
- Reemplazando expresamente esta DPC 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 ante los terceros de confianza

Sin limitar otras obligaciones del Suscriptor establecidas en esta DPC, los Suscriptores son responsables de cualquier tergiversación que hagan en los certificados a los terceros de confianza.

9.17.2. Deber de vigilar a los agentes

El Suscriptor controlará y será responsable de los datos que sus agentes proporcionen a Sectigo. El Suscriptor debe notificar de inmediato al emisor de cualquier tergiversación u omisión realizada por un agente. El deber de esta sección 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 secretas (elementos distribuidos) 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 realizarán ingeniería inversa en la implementación técnica de los servicios de la PKI cualificada de Sectigo, incluido el proceso de generación de claves, el sitio web público y los repositorios de Sectigo, excepto según lo permitido explícitamente por esta DPC o por aprobación de Sectigo mediante un escrito previo. 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 que aún no se haya pagado en virtud del acuerdo. El incumplimiento de esto como tercero de confianza resultará en la terminación del acuerdo con este 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 una PKI como una solución a sus requisitos de seguridad.

9.17.6. Limitaciones de las asociaciones de Sectigo

Los socios de la red de Sectigo no emprenderán acciones que puedan poner en peligro, poner en duda o reducir la confianza asociada a los certificados de Sectigo. Los socios de Sectigo se abstendrán específicamente de buscar asociaciones con otras autoridades raíz o aplicar procedimientos que se originen en dichas autoridades. El incumplimiento de esto resultará en la terminación del acuerdo con el socio, 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

A menos que se indique lo contrario en esta DPC, los Suscriptores serán exclusivamente responsables de:

- Minimizar el riesgo interno de compromiso de la clave privada asegurándose de que se proporcione internamente el conocimiento y la capacitación adecuados sobre PKI.
- Generar su propio par de claves privada / pública para usar en asociación con la solicitud de certificado enviada a Sectigo o a una RA externa de Sectigo para aquellos no emitidos dentro de un dispositivo hardware criptográfico (por ejemplo, un QSCD o HSM).
- Asegurarse de que la clave pública enviada a Sectigo o una RA de Sectigo corresponda con la clave privada utilizada para aquellas no emitidas dentro de un dispositivo hardware criptográfico (ej, QSCD o HSM).
- Asegurarse de que la clave pública enviada a Sectigo o a una RA de Sectigo sea la correcta para las que no se emitieron dentro de un dispositivo hardware criptográfico (ej, QSCD o HSM).

- Asegurarse de que las firmas digitales solo sean creadas por un dispositivo QSCD cuando los certificados se emitan dentro de un QSCD.
- Brindar información correcta y veraz en sus comunicaciones con Sectigo o una RA de Sectigo.
- Avisar a Sectigo o a una RA de Sectigo si en cualquier etapa mientras el certificado es válido, cualquier información enviada originalmente ha cambiado desde que fue enviada a Sectigo.
- Generar un nuevo par de claves seguras para usar en asociación con un certificado que solicite a Sectigo o a una RA de Sectigo para aquellos no emitidos dentro de dispositivos criptográficos hardware (ej, QSCD o HSM) realizado por Sectigo.
- Leer, comprender y aceptar todos los términos y condiciones de esta DPC de Sectigo y las políticas asociadas publicadas en el Repositorio de Sectigo.
- Abstenerse de manipular un certificado Sectigo.
- Utilizar los certificados de Sectigo para fines legales y autorizados de acuerdo con los usos y prácticas sugeridos en esta DPC.
- Dejar de usar un certificado de Sectigo si cualquier información que contenga se vuelve obsoleta o no válida.
- Dejar 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 digitales 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, que un suscriptor utiliza para generar, retener o destruir sus Claves Privadas.
- Usar la(s) clave(s) privada(s) para funciones criptográficas dentro del dispositivo criptográfico seguro cuando esté en QSCD o HSM.

Anexo A: Jerarquía y perfiles de CA cualificados

Jerarquía de personas físicas

Certificado raíz

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 29c39ebe521f1d39cf0bcad43ba5f33f ECDSA: 7e0aa94f2cbb01ea668b51e9e9423f57
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	Raíz de persona física cualificada Sectigo R / E45
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Validez (25 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Miércoles, 4 de octubre de 2045
Sujeto:	nombre común	Raíz de persona física cualificada Sectigo R / E45
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: eb5df65bb1c831e612f586d3fb77f10cdace7535 ECDSA: 21a43ad4c989cd31c5ec205d142d6e3e9d9db17b

Certificado de CA emisora

Persona física cualificada Sectigo CA R / E35

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 42211ba7e8e10a81d25da9bd8fd8120a ECDSA: 00c0721eeb06ad9b21780fa4db48c9db25
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	Raíz de persona física cualificada Sectigo R / E45
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Validez (15 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Jueves, 4 de octubre de 2035
Sujeto:	nombre común	Persona física cualificada Sectigo CA R / E35
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: 4fd206b1c19e54c35dd46d2fe49eb3b6984050e4 ECDSA: e53b95055f93030d965f2c9e629446628d146896

Jerarquía de personas jurídicas

Certificado raíz

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 20655a1b3ef150d79171ce6d8034ddbd ECDSA: 18ba1a9ac0ee669ffc9c703d032dc189
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	Persona jurídica cualificada Sectigo Raíz R / E45
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Validez (25 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Miércoles, 4 de octubre de 2045
Sujeto:	nombre común	Persona jurídica cualificada Sectigo Raíz R / E45

	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: 3155ebf15661313c0a98fa965d283d504f6eb6d4 ECDSA: 6bb7178f2ba92338a60d263cf63e6f269d922365

Certificado de CA emisora

Persona jurídica cualificada Sectigo CA R / E35

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 00d40b1204c9e4513275768b644f7a9df5 ECDSA: 00bf55b3b08ba28abad271e2ef2492b3c8
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	Persona jurídica cualificada Sectigo Raíz R / E45
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Validez (15 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Jueves, 4 de octubre de 2035
Sujeto:	nombre común	Persona jurídica cualificada Sectigo R / E35
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: 5e4a378921acc8ad49df63f1a5294cb6fac45853 ECDSA: 8bb032718459d725c3dc7a7eaa8ebaae8bf4455a

Jerarquía de CA web

Certificado raíz

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 01fd6d30fca3ca51a81bbc640e35032d ECDSA: 5c8b99c55a94c5d27156decd8980cc26
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	USERTrust Autoridad de certificación RSA / ECC
	Nombre de la Organización	USERTRUST
	localidad	Jersey City
	Estado o Provincia	New Jersey
	nombre del país	US
Validez:	No antes:	1 de febrero de 2010
	No después de:	18 de ene de 2038
Sujeto:	nombre común	USERTrust Autoridad de certificación RSA / ECC
	Nombre de la Organización	USERTRUST
	localidad	Jersey City
	Estado o Provincia	New Jersey
	nombre del país	US
Thumbprint		RSA: 2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E ECDSA: d1cbca5db2d52a7f693b674de5f05a1d0c957df0

Certificado de CA emisora

Autenticación de sitios web cualificada Sectigo CA R / E35

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 2762378048a1b3628d507e29220de220 ECDSA: 009e568d21ded89307c34080ff2d995901
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	USERTrust Autoridad de certificación RSA
	Nombre de la Organización	USERTRUST
	localidad	Jersey City
	Estado o Provincia	New Jersey
	nombre del país	US
Validez (15 años):	No antes:	Lunes, 5 de octubre de 2020
	No después de:	Jueves, 4 de octubre de 2035
Sujeto:	nombre común	Autenticación de sitios web cualificada Sectigo CA R / E35
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: 237014489151d07ce77a21061083d00fc5cf93f7 ECDSA: 9fc32441f3e04946432d86e81a99f96718b9738d

Autenticación de sitios web cualificada Sectigo CA Natural R / E35

Versión:	3 (0x2)	
Número de serie:	que contiene al menos 64 bits de salida de un CSPRNG	RSA: 0086380b2d3e65b9801030481e0e74362e ECDSA: 6866d57377f27657da8268a09e3faeb5
Algoritmo de firma:	sha384WithRSAEncryption o ecdsa-con-SHA384	
Editor:	nombre común	USERTrust Autoridad de certificación RSA
	Nombre de la Organización	USERTRUST
	localidad	Jersey City
	Estado o Provincia	New Jersey
	nombre del país	US
Validez (15 años):	No antes:	Martes, 17 de noviembre de 2020
	No después de:	Viernes, 16 de noviembre de 2035
Sujeto:	nombre común	Autenticación de sitios web cualificada Sectigo CA Natural R / E35
	Nombre de la Organización	Sectigo (Europe) SL
	nombre del país	ES
Thumbprint		RSA: 4ce9e54d353bd97238cf551f10a35aedddbe6504 ECDSA: d534700973d8d44ef041e47891d9a16482c657a4

Certificado END ENTITY

Ver documento de perfiles de certificado

Anexo B: Tipos de certificados cualificados Sectigo

Certificados cualificados sectigo para persona física

Ciudadano sectigo

Descripción	Dispositivo	Política	Sectigo OID	Firma / sello
Ciudadano	Sin QSCD	QCP-n	1.3.6.1.4.1.6449.1.2.1.7.1	Firma avanzada
Ciudadano	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.2	Firma cualificada

Empleado de Sectigo

Descripción	Dispositivo	Política	Sectigo OID	Firma / sello
Empleado	Sin QSCD	QCP-n	1.3.6.1.4.1.6449.1.2.1.7.3	Firma avanzada
Empleado	QSCD	QCP-n-qscd	1.3.6.1.4.1.6449.1.2.1.7.4	Firma cualificada

Certificados cualificados sectigo para persona jurídica

Sello de sectigo

Descripción	Dispositivo	Política	Sectigo OID	Firma / sello
Sello	Sin QSCD	QCP-l	1.3.6.1.4.1.6449.1.2.1.8.1	Sellado avanzado
Sello	QSCD	QCP-l-qscd	1.3.6.1.4.1.6449.1.2.1.8.2	Sellado cualificado

Sello Sectigo para PSD2

Descripción	Dispositivo	Política	Sectigo OID	Firma / sello
Certificado de sello para PSD2	Sin QSCD	QCP-l	1.3.6.1.4.1.6449.1.2.1.8.5	Sellado avanzado

Certificado de sello para PSD2	QSCD	QCP-l-qscd	1.3.6.1.4.1.6449.1.2.1.8.6	Sellado cualificado

Sectigo QWAC

Sectigo QWAC para persona jurídica

Descripción	Dispositivo	Política	Sectigo OID
QWAC para personas jurídicas	Sin QSCD	QCP-w	1.3.6.1.4.1.6449.1.2.1.8.3 1.3.6.1.4.1.6449.1.2.1.5.1

Sectigo QWAC para persona física

Descripción	Dispositivo	Política	Sectigo OID
QWAC para personas físicas	Sin QSCD	QCP-w	1.3.6.1.4.1.6449.1.2.1.7.5

Sectigo QWAC para PSD2

Descripción	Dispositivo	Política	Sectigo OID
QWAC para PSD2	Sin QSCD	QCP-w QCP-w-psd2	1.3.6.1.4.1.6449.1.2.1.8.4 1.3.6.1.4.1.6449.1.2.1.5.1

Anexo C: ChangeLog

Versión	Cambiar Descripción	Fecha
1.0	Nuevo DPC para certificados cualificados	Mayo de 2020
1.0.1	• Se eliminaron las secciones 1.6.3, 4.12, 4.9.4, 6.2.2, 6.2.3, 6.2.4 y 6.2.5 • Se eliminaron todas las secciones con "sin estipulación" • Se eliminó el EPKI y los socios potenciados de la sección 1.3.5 • Sección 3.2 reorganizada • Corrección algunos errores tipográficos y frases. • Se agregó una nueva sección 5.7.4	20 de agosto de 2020
1.0.2	• Especificó el procedimiento de identificación F2F o métodos equivalentes en la sección 3 • Sección 6.1.1 actualizada con respecto al monitoreo de QSCD • Eliminar las opciones de "nube" de los anexos	8 de septiembre de 2020
1.0.3	• Cambiar la dirección de la oficina de Barcelona • Explicado en la sección 6.3.2 qué se hace antes de que caduque un certificado de CA • Se modificó la sección 5.8 de terminación CA o RA a terminación TSP • Incluidas las auditorías internas realizadas cada 3 meses en el apartado 6.6.2	18 de septiembre de 2020
1.0.4	Adición de la información de CA en los anexos	5 de octubre de 2020
1.0.5	Agregar información de CA y certificados OID en los anexos	15 de octubre de 2020
1.0.6	Se actualizó la URL de la TSA cualificada	20 de octubre de 2020
1.0.7	• Actualización la sección 3.2.3.1.2 agregando nuevos métodos de validación para la verificación de IP • Aclaración sobre 3.1.5 sobre la unicidad de los nombres • Se actualizó la sección 4.2.4 agregando algunos otros dominios para la verificación de CAA • Actualización de errores tipográficos en las secciones 5.5.7 y 6.1.2 • Agregar requisitos de CABF sobre los motivos de revocación de CRL y OCSP en las secciones 7.2.2 y 7.3 • Corrección de tiempos en el Anexo A para certificados de CA	20 de octubre de 2020
1.0.8	Se actualizaron las CA: valor y el número de serie	22 de octubre de 2020
1.0.9	Corregir algunos errores tipográficos y actualizar la sección 5.4.7	22 de octubre de 2020
1.0.10	Se agregó un sello PSD2 en QSCD. OCSP y CRL actualizados con la adición de las extensiones archiveCutOff y ExpiredCertsOnCRL. Incluido un nuevo subCA para QWAC-n	3 de febrero de 2021
1.0.11	Sección 9.14.3 modificada y error tipográfico en 7.2	6 de abril de 2021

1.0.12	Agregar una nueva abreviatura y corregir algunos errores tipográficos Aclaraciones sobre los apartados 1 y 1.2 Eliminación de la sección 1.3.5.2 Sección 3.2.3 actualizada y aclarada Sección 4.9.9 actualizada Modificación en el período de retención de registros de 7 a 2 y actualización de la sección 5.4.3 Pequeño error tipográfico actualizado en 6.1.7 Sección 6.2.2 actualizada Sección 7.1.2.1 actualizada: - Se agregó la firma digital para la oración OCSP. - Indicó que el EKU no está presente en las CA raíz Sección 9.9 actualizada Bibliografía actualizada eliminando RFC 6844 y agregando 8659 Agregar otro OID de Sectigo en el Anexo B para QWAC-l y QWAC-l-PSD2	1 de abril de 2022
1.0.13	Actualización de la sección 1.5.2 para apuntar a nuestro sitio de revocación Aclaración sobre el respondedor OCSP en la sección 4.9.9 Se eliminó la información de medios extraíbles de la sección 5.4.3 y 5.4.4 Se actualizó la ejecución de análisis de vulnerabilidades de semanal a trimestral en la sección 5.4.7 Aclaración sobre el apartado 6.3.2 Actualización del apartado 7.1.2.1 y 7.1.2.2 respecto al bit de firma digital Sección 7.1.3 aclarada Sección 7.2.2 actualización de los códigos de motivo de la CRL Se actualizaron las secciones 4.9.1, 7.2 y 7.3 para hacer referencia también a los precertificados Se aclaró el último punto en la sección 9.6.2	30 de Septiembre de 2022
1.0.14	Actualización de la sección 1.1 para aclarar que Sectigo se adhiere a la última versión publicada de los documentos CABF Aclaración en la sección 2.4 sobre documentación Actualización de la sección 4.2.4 para registrar todas las acciones según los logs Aclaración sobre los sistemas de emisión en el apartado 4.3.1 Cambiado a 10 años el almacenamiento de CRL en la sección 4.9.6 Actualización en la sección 5.4.1 para incluir eventos de firewall y routers Añadida comunicación a terceros en el apartado 5.7.1 Aclaración del seguimiento de QSCD en la sección 6.1.1.1 Se agregó un punto adicional en la sección 6.1.1.2 para otras claves de CA Se incluye la conformidad con NetSec en la sección 6.7 Aclaración del EKU para subCAs en la sección 7.1.2.2	23 de Diciembre de 2022

	Clarificación indicando que Sectigo hace una comparación byte por byte del nombre del emisor en certificados de CA y de las CRLs en la sección 7.2.2 Actualización de la sección 9.6.1 para incluir violación de datos personales Actualización de la sección 9.17.7 sobre el uso de la clave privada en un QSCD	

Anexo D: Bibliografía

RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels

RFC 2253 - Lightweight Directory Access Protocol (v3) - UTF-8 String Representation of Distinguished Names

RFC 3161 - Internet X.509 Public Key Infrastructure - Time-stamp Protocol (TSP)

RFC 3279 - Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

RFC 3647 - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

RFC 5280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile

RFC 5754 – Using SHA2 Algorithms with Cryptographic Message Syntax

RFC 5758 – Internet X.509 Public Key Infrastructure - Additional Algorithms and Identifiers for DSA and ECDSA RFC 6844 - DNS Certification Authority Authorization (CAA) Resource Record

RFC 8659 – DNS Certification Authority Authorization (CAA) Resource Record

RFC 6960 - X.509 Internet Public Key Infrastructure - Online Certificate Status Protocol - OCSP

RFC 6962 - Certificate Transparency

ETSI EN 319 401 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers

ETSI EN 319 411-1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates

ETSI EN 319 403 - Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 412-1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI EN 319 412-2 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons

ETSI EN 319 412-3 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons

ETSI EN 319 412-4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates

ETSI EN 319 412-5 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements

ETSI TS 119 495 - Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366

ETSI TS 119 312 - Electronic Signatures and Infrastructures (ESI); Cryptographic Suites

ANSI X9.79 - Public Key Infrastructure - Practices and Policy Framework

ITU-T X.500 - Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services

ITU-T X.503 - Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks

ITU-T X.520 - Information technology - Open Systems Interconnection - The Directory: Selected attribute types

ISO 3166-1 - Codes for the representation of names of countries and their subdivisions – Part 1: Country codes

ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - The Directory - Part 8: Public-key and attribute certificate frameworks"

ISO/IEC 15408 - Information technology - Security techniques - Evaluation criteria for IT security

ISO/IEC 17065 - Conformity assessment — Requirements for bodies certifying products, processes and services

FIPS PUB 140-2 - Security Requirements for Cryptographic Module NIST

SP 800-89 - Recommendation for Obtaining Assurances for Digital Signature Applications NIST

SP 800-56A - Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography