Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Declaración de Práctica de Certificación

(CPS_ACA_023)

Documento Público

CONTROL DE VERSIONES

Fecha	Versión	Descripción / Cambios Relevantes
27/03/2003	CPS_ACA_001.0	Versión inicial
02/03/2004	CPS_ACA_001.1	Corrección erratas, Modificación perfil de certificado extensiones AKI. Cambios en perfil certificado CA y perfil de CRL.
26/10/2004	CPS_ACA_002.0	Revisión general. Modificaciones para mejor adecuación a lo dispuesto en la Ley 59/2003 de Firma Electrónica y mayor claridad para suscriptores y usuarios.
17/08/2005	CPS_ACA_002.1	Actualización nuevo certificado raíz
13/03/2006	CPS_ACA_003.0	Adaptación nuevo entorno CPD
13/07/2006	CPS_ACA_004.0	Inclusión de los certificados de Persona Jurídica
24/10/2006	CPS_ACA_005.0	Inclusión de los certificados de Servidor Seguro
25/05/2007	CPS_ACA_006.0	Inclusión de los certificados de Persona Jurídica software
02/03/2009	CPS_ACA_007.0	Se incluye el fax como contacto Se detalla el procedimiento de renovación Se detalla el proceso de notificación de suspensión o revocación Se detalla el procedimiento de suspensión Inclusión de los certificados de Sello Electrónico
02/09/2009	CPS_ACA_008.0	Se incluye la CA Trusted que depende de nuestra jerarquía y con las políticas correspondientes
28/02/2010	CPS_ACA_009.0	Se incluye la política de certificados de persona jurídica software bajo la CA Trusted
01/10/2010	CPS_ACA_010.0	Se incluye la política de certificados de sello electrónico software bajo la CA Trusted
21/12/2010	CPS_ACA_011.0	Se incluye la política de certificado reconocido de personal de colegio profesional
01/10/2011	CPS_ACA_012.0	Se incluye la política de certificado reconocido de abogado europeo
11/03/2014	CPS_ACA_013.0	Se incluye una descripción de la Jerarquía PKI Se incluyen los Fingerprint las CAs intermedias 2014 Se elimina detalles del modelo de módulo Criptográfico Se incrementa la longitud de las claves de usuario a 2048 bits Corrección de erratas

13/04/2016	CPS_ACA_014.0	Se elimina la denominación de certificado reconocido para los certificados de Penalnet
27/06/2016	CPS_ACA_015.0	Se incluye nueva Jerarquía PKI, información nuevos certificados CAs Se alinea con eIDAS Adaptación de servicios reconocidos a cualificados Alta de nuevos servicio cualificado de Representante de Persona Jurídica Alta de nuevos servicio cualificado de Autorizado Alta de nuevos servicio cualificado de Autenticación de Sitios Web Baja de servicios de Persona Jurídica, Persona Jurídica en Software, Abogado Penalnet.
14/09/2016	CPS_ACA_016.0	Se incorporan modificaciones para su alineación con lo dispuesto en el artículo 24.4 del Reglamento 910/2014 (eIDAs)
03/05/2017	CPS_ACA_017.0	Se incluye procedimiento de revisión de la CPS Se incluye enlace de acceso a la PDS Se incluyen los parámetros de generación de la clave pública Se incluye el modo de validación de certificado con posterioridad al periodo de validez del certificado mediante OCSP
02/06/2020	CPS_ACA_018.0	Adecuación del documento a RFC 3647 Actualización punto 5 controles de seguridad físicos
31/05/2022	CPS_ACA_019.0	Cambio de plantilla del documento Eliminación de apartados duplicados con las Políticas de Certificación Adecuación legislativa Ley 6/2020, de 11 de noviembre Actualización acrónimos
21/03/2023	CPS_ACA_020.0	Revisión anual legislativa Actualización apartado 4.9.5 indicando que si una solicitud de revocación no se puede confirmar en 24 horas no revoca el certificado. Actualización apartado 5.8 informando cómo se proveerá la información del cese del servicio. Actualización de apartado 7.1 indicando que el tamaño de los campos puede ser superior a los establecidos en la RFC 5280. Actualización apartado 9.6.4 y Resumen de los derechos y obligaciones indicando la obligación del usuario de comprobar la TSL .

14/04/2023	CPS_ACA_021.0	Actualización apartado 5.7.3 con el mecanismo para proveer información de estado de revocación en caso de compromiso de clave y cese del TSP. Actualización apartado 5.8 con el mecanismo para proveer información de estado de revocación en caso de cese del TSP. Modificación apartado 4.9.1 incluyendo como motivo de revocación cambios de estado de un QSCD.
01/03/2024	CPS_ACA_022.0	Revisión anual Corrección erratas
7/10/24	CPS_ACA_023.3	Se incluye nueva Jerarquía PKI, información nuevos certificados CA's y nuevos perfiles de certificados. Revisión de erratas.

ÍNDICE

Resumen de los derechos y obligaciones fundamentales contenidos en esta Declaración de Prácticas de Certificación (CPS)

ESTE TEXTO ES UNA MERA SÍNTESIS DEL CONTENIDO COMPLETO DE LA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS). ACONSEJAMOS QUE LEAN SU TEXTO ÍNTEGRO Y LOS DEMÁS DOCUMENTOS AFINES PARA OBTENER UNA VISIÓN CLARA DE LOS OBJETIVOS, ESPECIFICACIONES, NORMAS, PROCESOS, DERECHOS Y OBLIGACIONES QUE RIGEN LA PRESTACIÓN DEL SERVICIO DE CERTIFICACIÓN.

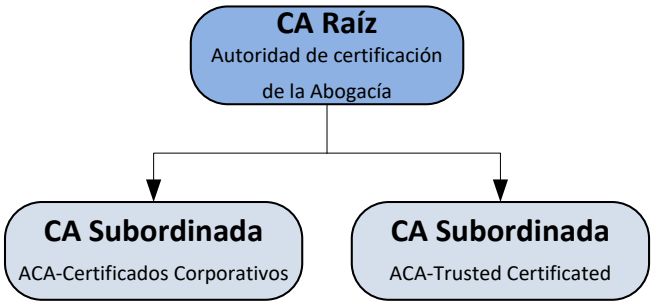
- Esta Declaración de Prácticas de Certificación (CPS) y los documentos afines regulan todo lo relativo a la solicitud, emisión, aceptación, renovación, reemisión, suspensión y revocación de certificados entre otros muchos aspectos vitales para la vida del certificado y el régimen jurídico que se establece entre el Solicitante/Suscriptor, la Autoridad de Certificación y Registro, y los Usuarios que confían en certificados y terceros.
- Tanto la Declaración de Prácticas de Certificación (CPS) como todos los demás documentos afines son puestos a disposición de futuros Solicitantes, Suscriptores y Usuarios en la dirección de Internet http://www.acabogacia.org/doc para que conozcan exactamente antes de contratar o confiar en AC Abogacía cuáles son las normas y reglas aplicables a nuestro sistema de certificación.
- AC Abogacía emite varios tipos de certificados, por lo que el Solicitante de un certificado deberá conocer las condiciones establecidas en la Declaración de Prácticas de Certificación (CPS) y en las correspondientes Políticas de Certificación de ese tipo de certificado, de manera que pueda proceder correctamente a la solicitud y uso del certificado.
- El Solicitante deberá solicitar el certificado correspondiente en la forma que se establece en el procedimiento determinado en la Declaración de Prácticas de Certificación (CPS) y documentos afines.
- Es imprescindible la custodia de las claves privadas que el Suscriptor debe hacer respecto de su certificado, pues si no toma las medidas adecuadas carecería de sentido el sistema de seguridad que se pretende implantar. En este sentido, es necesario informar inmediatamente a AC Abogacía cuando concurra alguna causa de revocación/suspensión del certificado establecidas en la Declaración de Prácticas de Certificación (CPS) y proceder, de esta manera, a su suspensión para evitar un uso ilegítimo del certificado por parte de un tercero no autorizado.
- El suscriptor deberá comunicar a AC Abogacía cualquier modificación o variación de los datos que se aportaron para conseguir el certificado, tanto si éstos aparecen en el propio certificado como si no.
- El Suscriptor debe hacer un uso debido del certificado, y será exclusiva responsabilidad suya la utilización del certificado de forma diferente a los usos previstos en la Declaración de Prácticas de Certificación (CPS) y los demás documentos afines.
- Es obligación ineludible del Usuario comprobar en el Depósito de Certificados publicado por AC Abogacía que el certificado en el que pretende confiar y el resto de los certificados de la cadena de confianza son válidos y no han caducado o han sido suspendidos o revocados.
- El usuario deberá comprobar por sus propios mecanismos, que la jerarquía con la que se encuentra emitido el certificado se encuentra en la lista de certificados cualificados de la unión europea (TSL).
- En la Declaración de Prácticas de Certificación (CPS) y documentos afines se establece la responsabilidad de AC Abogacía y de los Solicitantes, Suscriptores y Usuarios, así como la limitación de la misma ante la posible producción de daños y perjuicios.

1. Introducción

El Consejo General de la Abogacía Española (CGAE) es el órgano representativo, coordinador y ejecutivo superior de los Ilustres Colegios de Abogados de España y tiene, a todos los efectos, la condición de corporación de derecho público, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines.

El Consejo General de la Abogacía Española se constituye en Prestador de servicios de Confianza mediante la creación de una jerarquía PKI propia. En cumplimiento del Reglamento 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

La estructura general de la PKI de ACA está compuesta de dos niveles

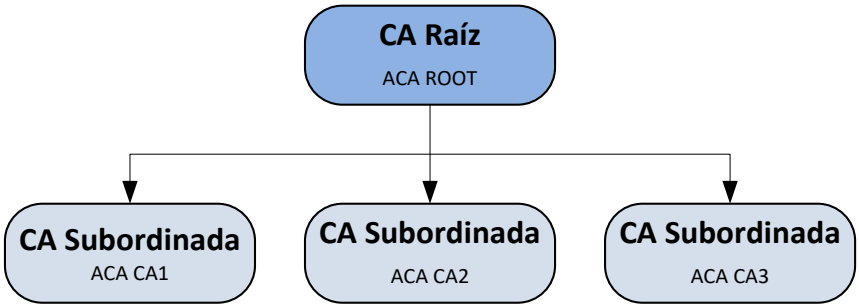


En el año 2014 fueron generadas nuevas CAs subordinadas con la misma denominación seguida del año de emisión: *ACA – Certificados Corporativos 2014 y ACA-Trusted Certificates 2014.*

Los certificados emitidos por ambas CAs subordinadas tienen continuidad con los mismos OID en las CAs versión de 2014.

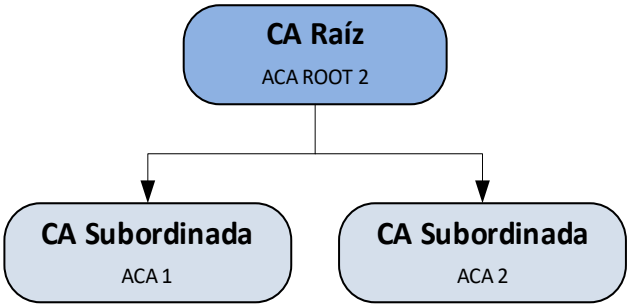
Por otro lado, en el año 2016 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente y se mantienen las descritas puesto que se encuentran en vigor los certificados expedidos por estas jerarquías. Se expedirán nuevos certificados mediante las nuevas CAs subordinadas.

Nueva Jerarquía 2016, compuesta de dos niveles:



En 2024 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente y se mantienen las descritas puesto que se encuentran en vigor los certificados expedidos por estas jerarquías. Se expedirán nuevos certificados mediante las nuevas CAs subordinadas.

Nueva Jerarquía 2024, compuesta de dos niveles;



1.1. Vista General

El presente documento especifica la Declaración de Prácticas de Certificación de la Autoridad de Certificación constituida por el Consejo General de la Abogacía Española, denominada Autoridad de Certificación de la Abogacía (AC Abogacía), para la emisión de certificados, y está basada en la especificación del estándar RCF 3647 – Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, de IETF.

La Declaración de Prácticas de Certificación (CPS) de la Autoridad de Certificación de la Abogacía que establece los términos concretos del servicio prestado se puede encontrar en http://www.acabogacia.org/doc.

Al ser AC Abogacia un Prestador privado de Servicios de confianza establecido en España l a normativa jurídica aplicable es la siguiente:

- REGLAMENTO (UE) 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, de aquí en adelante ReIDAS.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

El Consejo General de la Abogacía Española, como entidad reguladora de la abogacía, establece un sistema de certificación con el objeto de expedir certificados para diversos usos y diferentes usuarios finales. Por este motivo, se establecen tipos de certificados. Los certificados son expedidos a entidades finales, incluyendo colegiados, personal administrativo y de servicio, organizaciones y personas físicas que representan a dichas organizaciones, por Autoridades de Certificación del CGAE.

Esta Declaración de Prácticas de Certificación (CPS) está en conformidad con las políticas de certificación relativas a los diferentes certificados emitidos por AC Abogacía y que se identifican en el apartado “Ámbito de Aplicación y Usos” de esta Declaración de Prácticas de Certificación (CPS). En caso de contradicción entre los dos documentos prevalecerá lo dispuesto en las políticas de certificación concretas de cada tipo de certificado emitido.

La AC Abogacía, regida por esta Declaración de Prácticas de Certificación (CPS) y por las políticas citadas, establece la emisión de los siguientes tipos de certificados:

1. Servicio de expedición de certificados electrónicos cualificados de firma electrónica (QCP-n-qscd y QCP-n)
2. Servicio de expedición de certificados electrónicos cualificados de sello electrónico (QCP-l)

Los certificados cualificados lo son de acuerdo con lo establecido en el art. 28 de ReIDAS, siendo obligatorio la utilización de un dispositivo cualificado de creación de firmas electrónicas que cumple las definiciones del art. 51 de ReIDAS para la generación y custodia de los datos de creación de firma del suscriptor, y la creación de firmas.

Adicionalmente, y para un uso exclusivamente interno de soporte a las operaciones del sistema de gestión de la AC y las AR, se emitirán una serie de certificados específicos asociados a los diferentes roles de administración y operación, así como certificados que permiten la comunicación segura entre los diferentes componentes técnicos del sistema. Estos certificados constituyen simplemente un elemento

técnico necesario para la correcta y segura gestión del ciclo de vida de las clases de certificados anteriormente mencionados.

Esta Declaración de Prácticas de Certificación (CPS) define la forma en que la AC Abogacía da respuesta a todos los requerimientos y niveles de seguridad impuestos por las políticas de certificación.

En lo que se refiere al contenido de esta Declaración de Prácticas de Certificación (CPS), se considera que el lector conoce los conceptos básicos de PKI, certificación y firma digital, recomendando que, en caso de desconocimiento de dichos conceptos, el lector se informe a este respecto.

1.2. Identificación del documento

Nombre:	CPS_ACA_023
OID	1.3.6.1.4.1.16533.10.1.1
Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Versión:	023.3
Fecha de Emisión:	**7/10/24**
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación

1.3.1. Autoridad de Certificación (AC)

La entidad responsable de la emisión, y gestión de los certificados digitales es el Consejo General de la Abogacía Española (CGAE), que constituye un sistema de certificación bajo el nombre AC Abogacía y con una jerarquía PKI propia.

La jerarquía de CGAE está compuesta por:

AC Root y AC ROOT 2, son las Autoridades de Certificación de primer nivel. Sólo emiten certificados para sí misma y sus AC Subordinadas, certificado de validación de OCSP y la emisión de la ARL. Únicamente estará en funcionamiento durante la realización de las operaciones para las que se establece. La información más relevante del certificado:

Nombre Distintivo	CN = ACA ROOT, SERIAL NUMBER = Q2863006I, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Número de serie	47 43 91 24 3f ce c3 0d 57 48 28 6b ee 80 5d ab
Periodo de validez	Desde viernes, 27 de mayo de 2016 Hasta lunes, 27 de mayo de 2041
Huella Digital (SHA1)	d496592b305707386cc5f3cdb259ae66d7661fca
Huella Digital (SHA256)	97f654859cbde586fd90311e82ec7902c238cba0d6e529564

	c9c88f44895ec50
Huella Digital (SHA512)	eabb682b4764d41b4eebcdf35eccb65ed8f8a4b48d674aa35 a16f08c90422d717de175073d36aeaefa1b1d762108c41b94 c116c5100e4efae6e0a644c865bc66

Nombre Distintivo	CN = ACA ROOT 2, O = CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA, OI = VATES-Q2863006I, C = ES
Número de serie	049158150495b4ec3da98f78fc465c419c2296cf
Periodo de validez	Desde lunes, 18 de marzo de 2024 Hasta domingo, 18 de septiembre de 2044
Huella Digital (SHA1)	3a09eccf9d8770c3d5515806a9230ec9b32659be
Huella Digital (SHA256)	bd82b3dd8409362131614dc2058693efa67056d98b935bc5f597e50fe93cd947
Huella Digital (SHA512)	de44795ebb42223cb6af613c87d22a7efce16ee64723654060bef7c75255c69f939fef27508ad099a31bdffb8e54aeab27d8c36527f5a0eb9eb31ff114b1efd6

ACs Subordinadas: Son las Autoridades de Certificación subordinadas de “ACA CA ROOT” y “AC ROOT 2”, para la emisión de certificados finales, emisión del certificado de validación de OCSP y la emisión de la CRL. Esta es la información más relevante:

Nombre Distintivo	CN = ACA CA1, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Número de serie	49 1e f8 c2 bf 47 24 d3 57 6b d1 81 fc 67 05 ad
Periodo de validez	Desde jueves, 23 de junio de 2016 Hasta domingo, 23 de junio de 2030
Huella Digital (SHA1)	53d27de605858349fa2bd581d386407eee732517
Huella Digital (SHA256)	705eb3a0b1f09deda3ed45766bbbc02197700abb1e2d1d9e2862ac589dc9fd77
Huella Digital (SHA512)	476b08aa3c2c1095eb1a131a08f67a4aba11950fec224fba7f3a665c13dc858087d0f1b981ecac5aa457d73d2de4af5b4f659b51f524b98dc02c3b2719612b42

Nombre Distintivo	CN = ACA CA2, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Número de serie	49 a9 1d a5 cd 0d 70 c3 57 6b d1 1e 00 9d 55 dd
Periodo de validez	Desde jueves, 23 de junio de 2016 Hasta domingo, 23 de junio de 2030
Huella Digital (SHA1)	5c4df5ddc8e269a35d26ec18e14402f109b25030
Huella Digital (SHA256)	7e9316a5cecfb90a53adc3c7769450f42cdc3a9b85df4c7577b 053dcbb255812
Huella Digital (SHA512)	87266affec18817227c786842b1d591650ed7f6d84226dff651 fefbe48efacbedc12c6a69427a1b3c4eb23863197e72edb00aa a0d26edffc1f760aa636c91d89

Nombre Distintivo	CN = ACA CA3, OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, O = CONSEJO GENERAL DE LA ABOGACIA, C = ES
Número de serie	56 0f 1e 56 a6 30 b0 d4 57 6b cf e9 0f ba 2c eb
Periodo de validez	Desde jueves, 23 de junio de 2016 Hasta domingo, 23 de junio de 2030
Huella Digital (SHA1)	58490a3f3ecc96d08759ed2b091f28f13b2afaac
Huella Digital (SHA256)	af57fd805a0ef90e975765c0d5d55e3fd24cfc49 b73aa1a49e1979018d54fc26
Huella Digital (SHA512)	764c7061fb3d76dbc61c3431c08353e7ffda79db aedaab1b7142bfe8490efa97ad24f94bcb495fa9 b1b70b9c728ad7a7de37a3a9646bde38cc4d9717 ce4ef443

Nombre Distintivo	CN = ACA 1, O = CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA ,OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, C = ES
Número de serie	534f8eeb4149de83477ec5c5633029206e6b8955
Periodo de validez	Desde lunes, 18 de marzo de 2024 Hasta viernes, 18 de marzo de 2044

Huella Digital (SHA1)	2d221fe8039a1a80eeb21927b336f07b5643bd76
Huella Digital (SHA256)	c6dfaaace235da93e1c87d4ec7768652563d54c538b31e8cbd0680e91db75316
Huella Digital (SHA512)	db98f72977245524c9e36261e78d8af863649d5f21707811c530c3aa56c8fd8b54c28f400cfaf8958569f65810011c2930592855c93d1e85eb31f4098b83e7b1

Nombre Distintivo	CN = ACA 2, O = CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA ,OI = VATES-Q2863006I, OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA, C = ES
Número de serie	3705a42c126781af5737c3fba240e022d1dfe361
Periodo de validez	Desde lunes, 18 de marzo de 2024 Hasta viernes, 18 de marzo de 2044
Huella Digital (SHA1)	e136ab32d205b1249eaf032d78d293ad0a1b3acc
Huella Digital (SHA256)	dea1d4d5422ccec8364a58a8e6d221fdbe1673246b335438671f67a86017efdc
Huella Digital (SHA512)	a2b85231713f2463f7abe66211140b23de5e94d86d72338112172b74dafa7185987ab53483dffb3b1958a0fa82bd716915d71de7172010c87853c31796d48d96

La información relativa a la AC puede encontrarse en la dirección web www.acabogacia.org.

1.3.2. Autoridad de Registro (AR)

A los efectos de la presente Declaración de Prácticas de Certificación (CPS) podrán actuar como Autoridades de registro de los certificados las siguientes entidades:

a) El Consejo General de la Abogacía Española (CGAE)

b) Los Consejos Autonómicos de la Abogacía

c) Los Colegios de Abogados (registradores exclusivos para el Certificado de Colegiado)

d) Cualquier otra entidad delegada por la AC previa firma de contrato

En el territorio Español, sólo los Colegios de Abogados pueden ser Registradores para sus colegiados, debido a que los Colegios de Abogados poseen la capacidad certificadora en exclusiva, acerca de la condición de abogado.

1.3.3. Suscriptor

Es la persona física o jurídica a favor de la que se emite el certificado, e identificada en el nombre distinguido (DN) x501 del mismo. En el caso de los certificados cualificados emitidos a una persona física,

el suscriptor puede recibir también el nombre de "Firmante". En el caso de certificados cualificados emitidos a una persona jurídica, el suscriptor recibe también el nombre de "creador de sello".

El detalle de los suscriptores para cada tipo de certificado está definido en cada Política de Certificación.

1.3.4. Usuario

En esta Declaración de Prácticas de Certificación (CPS) se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el Certificado de AC Abogacía. el detalle de los usuarios para cada tipo de certificado está definido en cada Política Certificación.

1.3.5. Otros participantes

No estipulado

1.4. Ámbito de Aplicación y Usos

La presente Declaración de Prácticas de Certificación (CPS) da respuesta a las siguientes políticas de certificación, que se pueden encontrar en www.acabogacia.org/doc

En aquellos apartados, en los que los requisitos difieran entre una jerarquía de certificación y otra, siempre se hará una referencia expresa a ACA ROOT o ACA ROOT 2. Cuando no se haga distinción, aplicará a ambas.

- Jerarquía ACA ROOT

Política de Certificado Cualificado de Colegiado QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.10.2.1)	QCP-n-qscd
Política de Certificado Cualificado de Personal Administrativo QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.10.3.1)	QCP-n-qscd
Política de Certificado Cualificado de Representante de Persona Jurídica QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.10.10.1)	QCP-n-qscd
Política de Certificado Cualificado de Sello Electrónico (OID 1.3.6.1.4.1.16533.20.3.1)	QCP-l
Política de Certificado Cualificado de Personal de Colegio de Profesional QSCD en Tarjeta	QCP-n-qscd

(OID 1.3.6.1.4.1.16533.20.4.1)	
Política de Certificado Cualificado de Abogado Europeo QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.10.9.1)	QCP-n-qscd
Política de Certificado Cualificado "The Law Society of Scotland Qualified Certificates" QSCD en tarjeta (OID 1.3.6.1.4.1.16533.20.5.1)	QCP-n-qscd
Política de Certificado Cualificado de "Autorizado" QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.20.6.1)	QCP-n-qscd

- ACA ROOT 2

Política de Certificado Cualificado de Colegiado QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.50.1.1)	QCP-n-qscd
Política de Certificado Cualificado de Colegiado Software (OID 1.3.6.1.4.1.16533.50.1.3)	QCP-n
Política de Certificado Cualificado de Personal Administrativo QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.50.2.1)	QCP-n-qscd
Política de Certificado cualificado de personal administrativo Software (OID 1.3.6.1.4.1.16533.50.2.3)	QCP-n
Política de Certificado Cualificado de Representante de Persona Jurídica QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.50.3.1)	QCP-n-qscd
Política de Certificado Cualificado de Representante de Persona Jurídica Software (OID 1.3.6.1.4.1.16533. 50.3.3)	QCP-n
Política de Certificado Cualificado de Abogado Europeo QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.50.4.1)	QCP-n-qscd
Política de Certificado Cualificado de Abogado Europeo Software	QCP-n

(OID 1.3.6.1.4.1.16533.50.4.3)	
Política de Certificado Cualificado de "Autorizado" QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.50.5.1)	QCP-n-qscd
Política de Certificado Cualificado de "Autorizado" Software (OID 1.3.6.1.4.1.16533.50.5.3)	QCP-n
Política de Certificado Cualificado de Persona Física Software (OID 1.3.6.1.4.1.16533.50.6.3)	QCP-n
Política de Certificado Cualificado de Sello Electrónico (OID 1.3.6.1.4.1.16533.50.7.1)	QCP-l
Política de Certificado Cualificado de Personal de Colegio de Profesional QSCD en Tarjeta (OID 1.3.6.1.4.1.16533.60.1.1)	QCP-n-qscd
Política de Certificado Cualificado de Personal de Colegio de Profesional Software (OID 1.3.6.1.4.1.16533.60.1.3)	QCP-n
Política de Certificado Cualificado "The Law Society of Scotland Qualified Certificates" QSCD en tarjeta (OID 1.3.6.1.4.1.16533.60.2.1)	QCP-n-qscd
Política de Certificado Cualificado "The Law Society of Scotland Qualified Certificates" Software (OID 1.3.6.1.4.1.16533.60.2.3)	QCP-n

1.4.1. Usos permitidos de los certificados

Los certificados de AC Abogacía podrán usarse en los términos establecidos por las políticas de certificación correspondientes.

1.4.2. Usos Prohibidos y no Autorizados

Se prohíbe el uso de los certificados según lo dispuesto en la Declaración de Prácticas de Certificación (CPS) y las políticas de certificación específicas correspondientes.

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco

se permite la utilización distinta de lo establecido en las Políticas y en la Declaración de Prácticas de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

Los certificados de entidad final no pueden emplearse para firmar en el sistema peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC o CRL).

No están autorizadas las alteraciones en los Certificados, que deberán utilizarse tal y como son suministrados por la AC.

En el ámbito de los certificados cualificados QSCD en tarjeta, ni la AC ni las ARs crean, almacenan ni poseen en ningún momento la clave privada del suscriptor de certificados Cualificados, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor.

El Suscriptor o el Usuario que decida cifrar información lo hará en todo caso bajo su propia y única responsabilidad, sin que, en consecuencia, La AC tenga responsabilidad alguna en el caso de encriptación de información usando las claves asociadas al certificado.

1.5. Administración de la Política

1.5.1. Organización responsable

Autoridad de Certificación de la Abogacía.

Consejo General de la Abogacía Española.

1.5.2. Persona de contacto

Departamento Jurídico del Consejo General de la Abogacía Española

E-mail:	info@acabogacia.org
Teléfono:	915 23 25 93
Fax	915327836
Dirección:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

1.5.3. Responsable de la adecuación de las Prácticas y Políticas de certificación

El Consejo General de la Abogacía Española será el responsable de la correcta adecuación de las Políticas y Prácticas de Certificación

1.5.4. Procedimientos de aprobación de la Política

La publicación de las revisiones de esta Declaración de Prácticas de Certificación (CPS) deberá ser aprobada por AC Abogacía, después de comprobar el cumplimiento de los requisitos establecidos por el Consejo General de la Abogacía Española.

1.6. Definiciones y Acrónimos

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónico CA (*Certification Authority*)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónico RA (*Registration Authority*)
ARL	*Authority Revocation List*, lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española
CPS	*Certification Practice Statement*, Declaración de Practicas de Certificación. también puede encontrarse identificada por el acrónico DPC
CRL	*Certificate revocation list*, Lista de certificados revocados
CSR	*Certificate Signing request*, petición de firma de certificado
DES	*Data Encryption Estándar*. Estándar de cifrado de datos
DN	*Distinguished Name*, nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm*. Estándar de algoritmo de firma
DSCF/ **DCCFE**	Dispositivo Seguro de Creación de Firma Dispositivo Cualificado de Creación de Firmas Electrónicas
ReIDAS	Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
FIPS	*Federal information Processing Estandar publication*
IETF	*Internet Engineering task force*
ICA	Ilustre Colegio de Abogados
ISO	*International Organisation for Standardization*. Organismo intenacional de estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones.
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso directorio
OCSP	*On-line Certificate Status Protocol*. Protocolo de acceso al estado del Certificado

OID	*Object identifier*. Identicador de Objeto
PA	*Policy Authority*. Autoridad de la Política
PC	Política de Certificación puede encontrarse identificada por el acrónico CP (Certification Policy)
PIN	*Personal Identification Number*, Número de identificación personal
PKI	*Public Key Infrastructure*, Infraestructura de clave pública
PUK	*Personal Unblocking Key*, Código de desbloqueo
RSA	*Rivest-Shimar-Adleman*. Tipo de algoritmo de cifrado
SHA-256	*Secure Hash Algorithm*. Algoritmo seguro de Hash
TLS	*Transport Layer Security. Su antecesor es SSL(*protocolo diseñado por Netscape y convertido en estándar en la Red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor)
TCP/IP	Transmission Control Protocol/Internet Protocol Sistema de Protocolos, definidos en el marco de la IETFT. El Protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino, el Protocolo IP se encargará de direccional adecuadamente la información hacia su destinatario.
ENS	Esquema Nacional de Seguridad tiene por objeto determinar la política de seguridad en la utilización de medios electrónicos de las entidades de su ámbito de aplicación, estando constituido por los principios básicos y requisitos mínimos que garantizan adecuadamente la seguridad de la información tratada y los servicios prestados por dichas entidades. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
LOPD-GDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Publicación y Repositorio de Certificados

2.1. Repositorios

AC Abogacía podrá a disposición de los usuarios la siguiente información:

- Las Prácticas y Políticas de Certificación en la web www.acabogacia.org/doc
- Los términos y condiciones del servicio.
- Certificados emitidos.
- Certificados de las Autoridades de Certificación
- Certificados revocados e información sobre la validez de los certificados
- El documento "PKI Disclosure Statement"(PDS) en el siguiente sitio de Internet http://www.acabogacia.org/doc/EN

2.2. Repositorio de certificados

Se podrá acceder a los certificados emitidos, siempre que el suscriptor dé su consentimiento para que su certificado sea accesible, en el sitio de Internet http://www.acabogacia.org.

Se mantendrá un repositorio de todos los Certificados emitidos, durante el periodo de vigencia de la entidad emisora.

La AC mantendrá un sistema seguro de almacén y recuperación de certificados y un registro de certificados emitidos y su estado, pudiendo delegar estas funciones en una tercera entidad. El acceso al registro de certificados se realizará desde la web de AC Abogacía (www.acabogacia.org), o a través de otro canal que la AC considere seguro.

Una copia de las Prácticas y Políticas de Certificación estará disponible en formato electrónico en la dirección de Internet: http://www.acabogacia.org/doc . Las versiones anteriores podrán ser retiradas de su consulta on-line, pero pueden ser solicitadas por los interesados en AC Abogacía.

Los usuarios pueden solicitar una copia de la Declaración de Prácticas de Certificación (CPS) en formato papel en la dirección de contacto de AC Abogacía.

2.3. Frecuencia de publicación

AC Abogacía publicará de forma inmediata cualquier modificación en las políticas y prácticas de certificación, manteniendo un histórico de versiones.

AC Abogacía publicará los certificados en el registro de certificados inmediatamente después de haber sido emitidos.

La AC publicará una lista de certificados revocados de oficio con una periodicidad de 24 horas. AC Abogacía publicará de forma extraordinaria una nueva lista de revocación en el momento en que tramita una petición de suspensión o revocación autenticada.

2.4. Controles de acceso

AC Abogacía empleará diversos sistemas para la publicación y distribución de certificados y CRL's. Se necesitará tener unos datos de acceso para realizar consultas múltiples.

En la web de AC Abogacía existirán accesos al directorio para la consulta de CRL y Certificados bajo el control de una aplicación y protegiendo la descarga indiscriminada de información.

Las CRL's podrán descargarse de forma anónima mediante protocolo http desde las direcciones URL contenidas en los propios certificados en la extensión "CRL Distribution Point".

3. Identificación y Autenticación

3.1. Gestión de nombres

3.1.1. Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.501.

Los DN de los certificados ACA contendrán los elementos establecidos en cada Política de Certificación.

3.1.2. Significado de los nombres

Los nombres incluidos en los certificados serán significativos y comprensibles.

Los certificados de prueba se emitirán, por defecto, con los siguientes datos identificativos cuando aplique:

- Número de Documento Nacional de Identidad (DNI): 00000000T
- Número de Identidad de Extranjero (NIE): X0000000T, Y0000000R, Z0000000W
- Nombre: Nombre
- Primer apellido: Apellido1
- Segundo apellido: Apellido2

En caso necesario, se podrán generar certificados de prueba con otros datos habiendo informado previamente al Organismo correspondiente.

3.1.3. Pseudónimos

En ningún caso se pueden emplear nombres anónimos. Tampoco se pueden emplear pseudónimos para identificar a una organización.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

AC Abogacía atiende en todo caso a lo marcado por el estándar X.500 de referencia en la ISO/IEC 9594.

3.1.5. Unicidad de los nombres

Los nombres distinguidos de los certificados emitidos serán únicos para cada suscriptor. La AC se reserva la facultad de no emitir un certificado con el mismo nombre que uno ya emitido a otro suscriptor. El atributo del e-mail, el número de colegiado o el NIF se usan para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La AC no tiene responsabilidad en el caso de resolución de disputas de nombres. La AC no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver

disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

La AC se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

La asignación de nombres se realizará basándose en su orden de entrada.

La AC en todo caso se atiene a lo dispuesto en el apartado 9.13 de esta Declaración de Prácticas de Certificación (CPS).

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

La AC no asume compromisos en la emisión de certificados respecto al uso por los suscriptores de una marca comercial. AC Abogacía no permite deliberadamente el uso de un nombre cuyo derecho de uso no sea propiedad del suscriptor. Sin embargo la AC no está obligada a buscar evidencias de la posesión de marcas registradas antes de la emisión de los certificados.

3.2. Validación inicial de la identidad

3.2.1. Métodos de prueba de la posesión de la clave privada

Según lo dispuesto en cada Política de Certificación para ACA ROOT.

Para ACA ROOT 2, en los certificados cualificados QSCD en tarjeta, la clave privada será generada por el suscriptor y permanecerá en todo momento en posesión exclusiva del mismo.

En este caso, la AR hace entrega (si no dispone de él) de un kit conteniendo el dispositivo cualificado de creación de firmas electrónicas. Si el dispositivo no ha sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo cualificado de creación de firmas electrónicas. Durante este proceso se generan los datos de activación de del dispositivo, o si la inicialización se produce en una entidad externa, le serán entregados mediante un proceso que asegure la confidencialidad de los mismos ante terceros. La inicialización del dispositivo elimina totalmente cualquier información previa contenida en el mismo.

A continuación, el suscriptor genera el par de claves y un CSR en su dispositivo cualificado de creación de firmas electrónicas, enviando por un canal seguro la clave pública junto con los datos verificados a la AC en formato PKCS10 u otro equivalente. La generación del par de claves exigirá la introducción correcta de los datos de activación del dispositivo, y la introducción de un código de identificación del dispositivo que lo relaciona con el suscriptor autorizado a utilizarlo.

Por tanto, el método de prueba de la posesión de la clave privada por el suscriptor será PKCS#10.

Para los certificados cualificados QSCD en tarjeta, la clave privada será generada por el suscriptor y permanecerá en todo momento en posesión exclusiva del mismo estando custodiada en un dispositivo cualificado de creación de firmas electrónicas requiriéndose para su uso los datos de activación que sólo el suscriptor conoce.

Para los certificados cualificados en Software, el par de claves se generan a petición del solicitante, una vez se ha personado, ha sido validado por la Autoridad de Registro y ha firmado el documento de conformidad con la emisión del certificado cualificado, en software.

Cuando el solicitante acceda al servicio de generación, el sistema informará al titular de que se le va a emitir su certificado y generará en ese momento su correspondiente clave privada.

Para los certificados cualificados en Software, la generación de la clave se realizará en software, estableciendo el titular su propia contraseña que únicamente el conocerá, de modo que se garantice el control exclusivo por su parte.

3.2.2. Autenticación de la identidad de una organización

Según lo dispuesto en cada Política de Certificación

3.2.3. Autenticación de la identidad de un individuo

Según lo dispuesto en cada Política de-Certificación.

3.2.4. Información de suscriptor no verificada

Según lo dispuesto en cada Política de Certificación.

3.2.5. Validación de las Autoridades de Registro

La AC deberá asegurar los siguientes aspectos en relación a las Autoridades de Registro que se establezcan:

- Que existe un contrato en vigor entre la AC y la AR, especificando los aspectos concretos de la delegación y las responsabilidades de cada agente.
- Que la identidad de los operadores de la AR ha sido correctamente comprobada y validada.
- Que los operadores de la AR han recibido formación suficiente para el desempeño de sus funciones. Qué como mínimo han asistido a una sesión de formación de operador.
- Se requerirá autorización expresa de un representante capacitado de la Autoridad de Registro para actuar como operador.
- Que la AR ha sido auditada por una entidad externa designada por la AC.
- Que la AR asume todas las obligaciones y responsabilidades relativas al desempeño de sus funciones.
- Que la comunicación entre la AR y la AC, se realiza de forma segura mediante el uso de certificados digitales.
- Que las ARs se comprometen a cumplir con los requerimientos generales de seguridad indicados por la AC.

3.2.6. Criterios de Interoperabilidad

No estipulado

3.3. Identificación y autenticación de renovación de certificados

3.3.1. Renovación ordinaria

Según lo dispuesto en cada Política de Certificación

3.3.2. Reemisión después de una revocación

La emisión de un nuevo certificado a un suscriptor tras la revocación del certificado previo se tratará como una nueva emisión En todo caso la AC se reserva la facultad de denegar la reemisión si la causa de la revocación corresponde a los casos de compromiso de la clave privada del suscriptor.

3.4. Identificación y autenticación de una solicitud de revocación

Pueden solicitar la suspensión o revocación de un certificado:

- El propio suscriptor, en cuyo caso deberá facilitar la clave de revocación que se le entregó junto con el certificado, o deberá identificarse ante la AR
- Los operadores autorizados de la AR del suscriptor.
- Los operadores autorizados de la AC o de la jerarquía de certificación.

En cualquiera de los dos últimos casos deberán concurrir las circunstancias que se establecen en el apartado correspondiente, y se procederá en la forma allí descrita a realizar y tramitar las solicitudes de revocación.

4. Requerimientos Operacionales del ciclo de vida del certificado

4.1. Solicitud de certificados

Según lo dispuesto en cada Política de Certificación.

4.2. Procedimiento de solicitud de certificados

Según lo dispuesto en cada Política de Certificación.

4.3. Emisión de certificados

Según lo dispuesto en cada Política de Certificación.

4.4. Aceptación de certificados

Según lo dispuesto en cada Política de Certificación.

4.5. Uso del par de claves y del certificado

Según lo dispuesto en cada Política de Certificación.

4.6. Renovación de certificados

Según lo dispuesto en cada Política de Certificación.

4.7. Renovación de certificados y claves

Según lo dispuesto en cada Política de Certificación.

4.8. Modificación de certificados

No está permitida la modificación de certificados una vez emitidos.

4.9. Suspensión y Revocación de certificados

La revocación de un certificado supone la pérdida de validez del mismo, y es irreversible.

La suspensión, a diferencia de la revocación, supone la pérdida de validez temporal de un certificado, y es reversible.

Cuando el prestador decida revocar un certificado, registrará su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud. La revocación será efectiva inmediatamente después de su publicación. Dada la naturaleza de cada servicio, CRLs y OCSP, existe la posibilidad de una pequeña desincronización que en ningún caso superará los cinco (5) minutos. Esto ha de tenerse en cuenta por terceros que necesiten llevar a cabo validaciones del estado de revocación de certificados emitidos por este PSC con las máximas garantías sobre la sincronización de la información de revocación.

La suspensión y revocación de certificados serán notificadas al suscriptor del certificado mediante un correo electrónico a la cuenta de correo que figura en el certificado suspendido o revocado en conformidad con el Reglamento 910/2014 (ReIDAS) y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

4.9.1. Causas de revocación de certificados

La revocación de un certificado podrá ser debida a cualquiera de las siguientes causas:

1. Circunstancias que afectan a la información contenida en el certificado

- Modificación de alguno de los datos contenidos en el certificado.
- Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
- Ya no cumple la política bajo la que fue expedido.
- Pérdida o cambio del suscriptor de la vinculación con la institución, en el caso de Certificados de Personal Administrativo

Esta causa de revocación podrá solicitarla el usuario pudiendo utilizar el código de revocación para ACA ROOT o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

2. Circunstancias que afectan a la seguridad de la clave privada de la CA o del certificado

- Compromiso de la clave privada o de la infraestructura o sistemas de la AC, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.
- Infracción, por parte de la AC o de la AR, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la Declaración de Prácticas de Certificación (CPS).
- Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor.
- Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor.
- El uso irregular del certificado por el suscriptor.
- El incumplimiento por parte del suscriptor de las normas de uso del certificado expuestas en las políticas, en la Declaración de Prácticas de Certificación (CPS) o en el instrumento jurídico vinculante entre la AC, la AR y el suscriptor.

La causa de revocación relativa a acciones que afectan a la CA raíz o intermedia solo podrá realizarla los administradores de la AC.

La causa de revocación relativa a certificados de usuarios podrá solicitarla el usuario pudiendo utilizar el código de revocación para ACA ROOT o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

3. Circunstancias que afectan a la seguridad o usabilidad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Se produzcan cambios en el estado de acreditación del dispositivo como dispositivo seguro de creación de firma (QSCD).
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación de la clave privada.

- El incumplimiento por parte del suscriptor de las normas de uso del dispositivo criptográfico expuestas en las políticas, en la Declaración de Prácticas de Certificación (CPS) o en el instrumento jurídico vinculante entre la AC, la AR y el suscriptor.

La causa de revocación relativa a acciones que afectan a al dispositivo criptográfico donde se custodian las claves de la CA raíz o intermedia solo podrá realizarla los administradores de la AC

La causa de revocación relativa a certificados de usuarios podrá solicitarla el usuario pudiendo utilizar el código de revocación para ACA ROOT o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

4. Circunstancias que afectan al suscriptor

- Manifestación expresa y univoca del suscriptor o tercero autorizado
- Finalización de la relación jurídica entre la AC, la AR y el Suscriptor.
- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al suscriptor, incluyendo la inhabilitación temporal del colegiado para el ejercicio profesional.
- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.
- Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la Declaración de Prácticas de Certificación (CPS) de la AC.
- La incapacidad sobrevenida, total o parcial.
- Por el fallecimiento del suscriptor.

La causa de revocación relativa a certificados de usuarios podrá solicitarla el usuario pudiendo utilizar el código de revocación para ACA ROOT o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas

5. Otras circunstancias

- La suspensión del certificado digital por un período superior al establecido en la Declaración de Prácticas de Certificación (CPS).
- Por resolución judicial o administrativa que lo ordene.
- Por la concurrencia de cualquier otra causa especificada en la Declaración de Prácticas de Certificación (CPS).

6. Así como las indicadas en la normativa de aplicación.

Las causas de revocación consecuencia de cualquiera esta circunstancia lo realizaran los Operadores autorizados de la AR o los Administradores de la AC, siempre que existan motivos fundados.

Si la AR o la AC a la que se dirige la solicitud de revocación no disponen de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión. Cuando el suscriptor tenga conocimiento de la suspensión del certificado deberá abstenerse de utilizarlo, y contactar con la AR o la AC para proceder a su revocación o al levantamiento de la suspensión, su hubiere lugar.

El instrumento jurídico que vincula a la AC y a la AR con el suscriptor establecerá que el mismo deberá solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

4.9.2. Quién puede solicitar la revocación

Pueden solicitar la revocación de un certificado:

- El propio suscriptor.
- Los operadores autorizados de la AR del suscriptor siempre que tenga motivos fundados.
- Los Administradores autorizados de la AC siempre que tenga motivos fundados de cualquiera de las circunstancias expuestas en el apartado 4.9.1 de la DPC.

4.9.3. Procedimiento de solicitud de revocación

El procedimiento de solicitud de revocaciones o suspensiones presenta puede iniciarse por vía presencial, telefónica, por correo electrónico u online para ACA ROOT, en la página web de AC Abogacía.

Procedimiento presencial:

- Solicitud por parte del suscriptor. El suscriptor acreditará su identidad ante un operador de su AR, y manifestará por escrito, su deseo de revocar suspender o revocar el certificado. El operador procederá a efectuar la suspensión o revocación, informando al suscriptor de la realización del trámite.
- Suspender por parte de un tercero: En el caso de ser un tercero el que manifiesta la solicitud, el operador le realizará una seria de preguntas para determinar la causa de la solicitud, recibirá la documentación pertinente, y si considera que concurren las causas establecidas procederá a efectuar la suspensión, una suspensión cautelar a la espera de más averiguaciones. Asimismo, enviará un mensaje al suscriptor comunicándole la circunstancia.

Procedimiento online para ACA ROOT:

El suscriptor de un certificado de Colegiado o de empleado dispondrá de una página web en www.acabogacia.org desde la que podrá solicitar la revocación de su certificado.

Para ello, deberá:

- Acceder a http://www.acabogacia.org
- Seleccionar: Revoca tu firma en la sección de zona de usuarios
- Introducir el Código de Revocación proporcionado durante el proceso de generación del certificado.

Al tiempo de revocarse el certificado, se notificará al suscriptor, comunicando motivos, fecha y hora en que el certificado quedará sin efecto.

El servicio de gestión de las revocaciones estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la AC, ésta realizará los mayores esfuerzos para asegurar que este servicio no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

La información relativa al estado de la revocación estará disponible las 24 horas del día, los 7 días de la semana. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la AC, ésta

realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

Para los certificados emitidos con la nueva jerarquía ACA ROOT 2, no se permitirá la solicitud de revocación online, estando habilitados los siguientes procedimientos además del presencial:

Por medio de correo electrónico con una disponibilidad de 24x7 o telefónicamente, las solicitudes de revocación de certificados deberán ser efectuadas según lo descrito a continuación:

- El suscriptor deberá comunicar la solicitud de revocación.
- El suscriptor y, en su caso, el responsable del certificado, pueden solicitar su revocación
- AC Abogacía contrastará los datos del cliente y bien vía telefónica o por correo electrónico solicitará la siguiente información:
    - Nombre
    - Apellidos
    - NIF
    - E-Mail y/o teléfono
    - Empresa u Organismo del certificado a revocar
    - Causa de revocación

En caso de que el suscriptor disponga de varios certificados, no se preguntará por uno en concreto, es el usuario el que debe de facilitar la empresa u organismo a la que pertenece el certificado a revocar.

- Validados estos datos y aceptada la solicitud de revocación, se procederá de carácter inmediato, a la revocación del certificado.
- Se comprobará que esta revocación ha sido efectuada correctamente, y que la CRL ha sido publicada y está disponible en el recurso Web. Contrastando en ella el número de serie del certificado y que ha sido firmada por la misma AC.
- Una vez revocado el certificado, se confirmará al firmante o suscriptor mediante el envío de un correo electrónico, que este ha sido revocado, al igual que la fecha desde la que ha dejado de ser efectivo y el motivo por el cual se ha revocado.

4.9.4. Periodo de gracia para la solicitud de revocación

La revocación se llevará a cabo de forma inmediata a la tramitación de cada solicitud verificada como válida. Por tanto, no existe ningún periodo de gracia asociado a este proceso durante el que se pueda anular la solicitud de revocación

4.9.5. Tiempo establecido para procesar una solicitud de revocación

Cuando el prestador decida revocar un certificado, registrará su revocación en su base de datos de certificados y publicarán el estado de revocación del certificado oportunamente y, en todo caso, en un plazo de 24 horas después de la recepción de la solicitud, siempre que la identidad del solicitante de la revocación haya sido autenticada según lo expuesto anteriormente, y la revocación debidamente tramitada por la AR, la revocación será efectiva inmediatamente después de su publicación.

4.9.6. Obligación de comprobación del estado de revocación por los usuarios

Los terceros que aceptan los certificados podrán verificar el estado de los mismos accediendo a los servicios de consulta sobre la vigencia de los certificados establecidos por AC Abogacía, dicha información de localización se encuentra en el propio certificado que se pretende verificar.

Los usuarios deben comprobar obligatoriamente el estado de los certificados en los cuales va a confiar, debiendo comprobar en todo caso la última CRL emitida, que podrá descargarse en las direcciones URL contenidas en el propio certificado, en la extensión "*CRL Distribution Point*".

La CRL está firmada por la autoridad de certificación que ha emitido el certificado. El usuario debe comprobar adicionalmente la(s) CRL(s) pertinentes de la cadena de certificación de la jerarquía.

El usuario deberá comprobar que la lista de revocación es la más reciente emitida ya que pueden encontrarse a la vez varias listas de revocación válidas. Los certificados incluyen la información necesaria para el acceso a la CRL.

El usuario deberá asegurarse que la lista de revocación está firmada por la autoridad que ha emitido el certificado que quiere validar.

4.9.7. Frecuencia de emisión de CRLs

La AC raíz de la jerarquía de certificación de AC Abogacía emitirá una CRL (ARL) cada vez que se revoca el certificado de una AC en la jerarquía. En todo caso emitirá una CRL (ARL) con una frecuencia mínima de 12 meses.

Las SubCAs de ACA emitirán una CRL cada 24 horas, o en su defecto, cada vez que exista una modificación del estado de un certificado de su jerarquía.

En particular, se emitirá una CRL nueva inmediatamente después de que se produzca un cambio en el estado de un certificado.

La AC mantendrá un histórico de CRL´s y ARL´s emitidas.

En el caso de emitirse la última CRL para la validación de los certificados de entidad final, se configurará el campo nextUpdate con el valor de "99991231235959Z", tal y como establece el estándar ETSI EN 319 411-1.

Por último, la Autoridad de Certificación de la Abogacía (AC ABOGACÍA), como prestador cualificado de servicios de confianza que expide certificados cualificados, proporcionará a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ella. Esta información deberá estar disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que sea fiable, gratuita y eficiente mediante el OCSP indicado en el certificado.

4.9.8. Tiempo de latencia máximo para las CRLs

La publicación de las CRLs será inmediata tras su emisión.

4.9.9. Disponibilidad de servicios de comprobación del estado de los certificados

La AC proporciona un servicio on-line de comprobación de revocaciones, el cual estará disponible las 24 horas del día los 7 días de la semana. La AC realizará todos los esfuerzos necesarios para que el servicio nunca se encuentre indisponible de forma continua más de 24 horas.

El usuario que no utilice los sistemas de validación de certificados habilitados a tal efecto para comprobar la validez de un certificado deberá consultar el Registro de Certificados para confiar en él.

Este plazo no será de aplicación para supuestos de fuerza mayor en los términos del artículo 1105 del Código Civil. Tampoco será de aplicación bajo los supuestos donde ACA no sea responsable incluyendo fuentes de alimentación eléctrica, comunicaciones, componentes de hardware y software del que ACA no sea titular o cualesquiera otras análogas.

4.9.10. Requisitos de la comprobación del estado de los certificados

Se dispone de un servicio de validación de certificados mediante el protocolo OCSP. Este servicio será de acceso libre y debe considerar:

- Comprobar la dirección contenida en la extensión AIA (Authority Information Access) del certificado.
- Comprobar que la respuesta OCSP está firmada. El certificado de firma de respuestas OCSP emitidos por AC Abogacia son conformes a la norma: RFC 6960 “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP”.
- El certificado de firma de las respuestas OCSP de la AC está emitido por la CA que emite el certificado que se quiere validar.

Para el uso del servicio de CRLs, que es de acceso libre, deberá considerarse que:

- Se deberá comprobar en todo caso la última CRL emitida, que podrá descargarse en la dirección URL contenida en el propio certificado en la extensión “CRL Distribution Point” o en esta misma PC como en la DPC.
- El usuario deberá comprobar adicionalmente las CRLs pendientes de la cadena de certificación de la jerarquía.
- El usuario deberá asegurarse que la lista de revocación esté firmada por la autoridad que ha emitido el certificado que quiere validar.
- Para ACA ROOT 2, los certificados revocados que expiren no serán retirados de la CRL, manteniendo estos durante quince (15) años para los certificados cualificados

4.9.11. Otras formas de divulgación de información de revocación disponibles

Sin estipulación.

4.9.12. Requisitos especiales de revocación por compromiso de las claves

En el caso de compromiso de las claves de la AC, el prestador cualificado de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento del incidente de seguridad, notificará al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el prestador de servicios de confianza notificará también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad.

4.9.13. Causas de suspensión de un certificado

La suspensión de certificados está contemplada únicamente para los certificados de ACA ROOT.

La suspensión, a diferencia de la revocación supone la pérdida de validez temporal de un certificado, y es reversible.

El período de suspensión se indicará claramente en la base de datos de certificados y el estado de suspensión será visible, durante el período de suspensión, a partir del servicio que proporcione la información sobre el estado del certificado.

La decisión de revocar o no un certificado suspendido será tomada por la AR o la AC en un periodo máximo de 30 días naturales. Durante este tiempo el certificado permanece suspendido.

AC Abogacía decide respecto al estado posterior a la suspensión del certificado (activo, si no procede la solicitud o revocado definitivamente) basándose en la información obtenida hasta ese momento respecto a las causas aducidas para la petición de revocación.

Si la AR o la AC a la que se dirige la solicitud de revocación no disponen de toda la información necesaria para determinar la revocación de un certificado, pero tiene indicios de su compromiso, puede decidir su suspensión.

La AC o la AR podrán suspender un certificado si se sospecha el compromiso de una clave, hasta que este hecho sea confirmado o desmentido.

Los certificados suspendidos aparecen en la CRL con causa de revocación “Certificate Hold (6)” (RFC 5280).

4.9.14. Quién puede solicitar la suspensión

Pueden solicitar la suspensión de un certificado de ACA ROOT:

- Los operadores autorizados de la AR del suscriptor siempre que tenga motivos fundados y como media preventiva
- Los Administradores autorizados de la AC siempre que tenga motivos fundados y como media preventiva.

4.9.15. Procedimiento para la solicitud de suspensión

El Suscriptor acudirá ante un Operador de una AR y pedirá que se solicite la suspensión como medida de precaución y durante un periodo de tiempo limitado.

Un tercero que contacte, por teléfono o de forma presencial, con un operador autorizado de ACA podrá solicitar la suspensión de un certificado, el Operador realizará una serie de preguntas para garantizar la legitimidad de la suspensión y procederá a suspenderlo y a contacta con el suscriptor del Certificado para actuar en consecuencia.

Al tiempo de suspenderse el certificado, se notificará al suscriptor, comunicando motivos, fecha y hora en que el certificado quedará sin efecto. Además indicará su duración máxima, extinguiéndose la vigencia del certificado si transcurrido dicho plazo no se hubiera levantado la suspensión.

No se producirá la suspensión de certificados cualificados de la jerarquía ACA ROOT 2

4.9.16. Límites del periodo de suspensión

El periodo máximo de suspensión de un certificado es de 30 días naturales.

4.10.Servicios de comprobación del estado de los certificados

4.10.1. Características operativas

AC Abogacía pondrá a disposición la información relativa al estado de sus certificados a través del servicio de OCSP.

Se facilitará también información sobre la suspensión o revocación de los certificados mediante la publicación periódica de las correspondientes CRLs.

La utilización del servicio OCSP es público y gratuito. La información sobre el estado de revocación o caducidad de los Certificados permite a los usuarios conocer el estado del Certificado, no solo hasta que éste expire, sino más allá de dicha fecha, a través del servicio de OCSP.

4.10.2. Disponibilidad del servicio

Los servicios de la consulta del estado de los certificados funcionarán 24 horas al día, 7 días a la semana y todos los días del año. En caso de fallo del sistema, o cualquier otro factor que no esté bajo el control de la CA, ésta realizará los mayores esfuerzos para asegurar que este servicio de información no se encuentre indisponible durante más tiempo que el periodo máximo de 24 horas.

4.10.3. Características adicionales

Sin estipulación.

4.11. Finalización de la suscripción

Se entenderá el fin de la suscripción del servicio cuando finalice el plazo de validez del certificado o cuando éste sea revocado.

4.12. Custodia y recuperación de clave

La clave privada de la AC raíz como las de las AC Subordinadas de AC Abogacía, han sido generadas sobre módulos de seguridad criptográficos, cumpliendo con niveles de seguridad necesarios.

AC Abogacía en ningún momento podrá recuperar la clave de los suscriptores. En caso de pérdida u olvido de la contraseña de acceso a las mismas, se deberá revocar el certificado y emitir uno nuevo.

En el ámbito de los certificados cualificados QSCD en tarjeta, ni la AC ni las ARs crean, almacenan ni poseen en ningún momento la clave privada del suscriptor, ni los datos de activación del dispositivo que la custodia, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor.

Para los certificados cualificados en Software, cuya generación y almacenamiento de la clave se haya realizado en software, la custodia será responsabilidad del suscriptor y éste será el responsable de mantenerla bajo su exclusivo control.

5. Controles de Seguridad Física, Procedimental y de Personal

5.1. Controles de Seguridad física

La AC tiene establecidos controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación de certificados ofrece protección frente:

- Accesos físico no autorizados
- Desastres naturales
- Incendios
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Inundaciones
- Robo
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del Prestador de Servicios de Certificación

Las instalaciones del centro de datos cumplen con las especificaciones TIER III y IV y cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

5.1.1. Ubicación y construcción

Los edificios donde se encuentra ubicada la infraestructura de la AC disponen de medidas de seguridad de control de acceso, de forma que solo se permite la entrada a los mismos a las personas debidamente autorizadas, los cuales cumplen los siguientes requisitos físicos:

- Ubicado en emplazamientos específicos para evitar daños por posibles incendios.
- Ausencia de ventanas al exterior del edificio.
- Cámaras de vigilancia en las áreas de acceso restringido.
- Controles de accesos basados en tarjeta y contraseña.
- Sistemas de protección y prevención de incendios.
- Protección del cableado contra daños e interceptación de la transmisión de datos

5.1.2. Acceso físico

El acceso físico a las dependencias del Prestador de Servicios de Certificación donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales.

Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro de este, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con personal privado de seguridad.

El acceso a las salas se realiza con lectores de tarjeta de identificación y gestionado por un sistema informático que mantiene un log de entradas y salidas.

5.1.3. Alimentación eléctrica y aire acondicionado

Los equipos informáticos de la AC están convenientemente protegidos ante fluctuaciones o cortes de suministro eléctrico, que puedan dañarlos o interrumpir el servicio.

Las instalaciones cuentan con un sistema de estabilización de la corriente, así como de un sistema de generación propio con autonomía suficiente para mantener este suministro durante el tiempo que requiera el cierre ordenado y completo de todos los sistemas.

Los equipos informáticos están ubicados en un entorno donde se garantiza una climatización (temperatura y humedad) adecuada a sus condiciones óptimas de trabajo.

Se realizan controles periódicos de los generadores y fuentes de energía para validar el correcto funcionamiento.

5.1.4. Exposición al agua

Las instalaciones donde se encuentran los equipos están protegidas para evitar las exposiciones al agua de los mismos, mediante detectores de humedad y otros mecanismos de seguridad.

Se realizan controles periódicos de estos elementos

5.1.5. Protección y prevención de incendios

Las instalaciones donde se encuentran los equipos de la AC, cuentan con las medidas adecuadas de protección contra el fuego, tales como detectores de humo sensores iónicos, alarmas, extintores y gas HFC-227 en caso de incendio.

Se realizan controles periódicos de todos estos elementos .

5.1.6. Sistema de almacenamiento.

Se han establecido los procedimientos necesarios para disponer de copias de respaldo de toda la información de su infraestructura productiva. Las copias de respaldo se almacenan de forma segura.

ACA dispone de planes de copia de respaldo, para toda la información sensible y de aquella considerada como necesaria para la persistencia de su actividad.

5.1.7. Eliminación de residuos

Cuando haya dejado de ser útil, la información sensible es destruida en la forma más adecuada al soporte que la contenga.

Impresos y papel: mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

Medios de almacenamiento: antes de ser desechados o reutilizados deben ser procesados para su borrado físicamente destruidos o hacer ilegible la información contenida.

5.1.8. Backup externo

La AC dispone de copias de seguridad en ubicaciones distintas que reúnen las medidas precisas de seguridad y con una separación física adecuada.

5.2. Controles procedimentales

Por razones de seguridad, la información relativa a los controles de procedimiento se considera materia confidencial y solo se incluye una parte de la misma. Asimismo, la AC garantiza que sus sistemas se operan y administran de forma segura, y para este propósito establece e implanta procedimientos para las funciones que afecten a la provisión de sus servicios.

5.2.1. Roles de confianza

Los roles de confianza son los que se describen en las respectivas Políticas de Certificación de la jerarquía de forma que se garantiza una segregación de funciones que disemina el control y limita el fraude interno, no permitiendo que una sola persona controle de principio a fin todas las funciones de certificación.

Según lo especificado en la norma CEN CWA 14167-1, se establecen los siguientes roles para:

Gestión del sistema:

- Responsable de Seguridad (Security Officer): Mantiene la responsabilidad global sobre la administración y la implementación de las políticas y procedimientos de seguridad
- Administradores del sistema de Certificación (System Administrators): Autorizado para realizar cambios en la configuración del sistema, pero sin acceso a los datos del mismo.
- Operadores de Sistemas (System Operator): Responsables de la gestión del día a día del sistema (Monitorización, backup, recovery,…)
- Auditor interno (System Auditor): Autorizado a acceder a los logs del sistema y verificar los procedimientos que se realizan sobre el mismo.
- Operador de CA – Operador de Certificación: Responsables de activar las claves de CA en el entorno Online.
- Operador de RA (Registration Officer): Responsables de aprobar, emitir, suspender y revocar los certificados de Entidad final

Gestión del HSM

- Administrador HSM Custodio del acceso, mediante dispositivo seguro (token), a las tareas administrativas del HSM.
- Operador HSM Acceso a la consola del HSM y de la habilitación del mecanismo de accesos mediante dispositivos seguros (token).
- Usuario HSM Custodio del acceso mediante dispositivo seguro (token) a la partición donde se aloja la clave privada de la AC.

5.2.2. Número de personas requeridas por tarea

La AC garantiza al menos tres personas, para realizar las tareas que requieran un control multi-persona detalladas a continuación:

- Generación de la clave de las ACs.
- Recuperación y backup de la clave privada de las ACs
- Emisión de certificados de las ACs.
- Activación de la clave privada de las ACs.
- Cualquier otra actividad realizada sobre los recursos hardware y software que dan soporte a la AC raíz.

5.2.3. Identificación y autentificación para cada rol

Las personas asignadas para cada rol son identificadas para asegurar que solo realiza las operaciones para las que está asignado a través de un auditor.

El acceso a los activos viene definido por estos roles, aportando a la vez, acceso a los mismos por medio de dispositivos seguros.

5.2.4. Roles que requieren separación tareas

La Autoridad de certificación de la Abogacía cumple con lo establecido en la norma CWA 14167-1 en relación a las siguientes incompatibilidades entre roles:

- Incompatibilidad entre oficial de seguridad y operador del HSM.
- Incompatibilidad entre los roles administrativos (administrador de sistema y operador de la AR).
- Incompatibilidad entre los administradores y los operadores del HSM.
- Incompatibilidad entre el rol auditor de sistema y cualquier otro rol

5.3. Controles de seguridad de personal

5.3.1. Requerimientos de antecedentes, calificación, experiencia, y acreditación

El personal que presta sus servicios en el ámbito de la Autoridad de Certificación posee el conocimiento, experiencia y formación suficientes, para el correcto cometido de las funciones asignadas. Para ello, la AC lleva a cabo los procesos de selección de personal que estima necesarios con objeto de que el perfil profesional del empleado se adecue lo más posible a las características propias de las tareas a desarrollar.

5.3.2. Procedimientos de comprobación de antecedentes

La AC realiza las investigaciones pertinentes antes de la contratación de cualquier persona. Estas prácticas aseguran los requisitos de experiencia, cualificación e historial precisos para cada puesto, sean o no de un rol de confianza.

5.3.3. Requerimientos de formación

Se provee al personal relacionado con la explotación de la AC de toda la información y documentación necesaria sobre los procedimientos operativos relativos a la misma.

Se supervisa la realización de la formación y grado de confianza por parte del personal y lleva a cabo los test necesarios para poder evaluar el nivel adecuado de conocimientos asimilados.

5.3.4. Requerimientos y frecuencia de la actualización de la formación

Los empleados de la AC y de las ARs realizan los cursos de actualización necesarios para asegurarse de la correcta realización de las tareas de certificación, especialmente cuando se realicen modificaciones sustanciales en las mismas y al menos con una frecuencia anual.

5.3.5. Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6. Sanciones por acciones no autorizadas

La AC y los PSC disponen de un régimen sancionador interno por la realización de acciones no autorizadas.

Se consideran acciones no autorizadas las que contravengan la Declaración de Prácticas de Certificación o las Políticas de Certificación pertinentes tanto de forma negligente como malintencionada.

5.3.7. Requerimientos de contratación de personal

Los empleados contratados para realizar tareas confiables deberán firmar anteriormente las cláusulas de confidencialidad y requerimientos operacionales empleados por la AC. Cualquier acción que comprometa la seguridad de los procesos críticos aceptados podrá dar lugar a sanciones.

5.3.8. Documentación proporcionada al personal

La AC pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas las políticas y prácticas que rigen dichos procesos y la documentación de seguridad.

Adicionalmente se suministrará la documentación que precise el personal en cada momento, al objeto de que pueda desarrollar de forma competente sus funciones.

5.4. Procedimiento de Auditoria de logs

5.4.1. Tipos de eventos registrados

AC Abogacía registra y guarda los logs de todos los eventos relativos al sistema de seguridad de la AC. Estos incluyen los siguientes eventos:

- Arranque y parada de aplicaciones.
- Intentos exitosos o fracasados de inicio y fin de sesión.
- Intentos exitosos o fracasados de crear, modificar o borrar usuarios del sistema autorizados.
- Los relacionados con la gestión del ciclo de vida de los certificados y CRLs.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados.
- Backup, archivo y restauración.
- Cambios en la configuración del sistema.
- Actualizaciones de software y hardware
- Cambios en los detalles de la AC y/o sus claves.
- Eventos asociados al uso del módulo criptográfico de la AC.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.

Las operaciones se dividen en eventos, por lo que se guarda información sobre uno o más eventos para cada operación relevante. Los eventos registrados poseen, como mínimo, la información siguiente:

- Categoría: Indica la importancia del evento.
    - Informativo: los eventos de esta categoría contienen información sobre operaciones realizadas con éxito.
    - Marca: cada vez que empieza y termina una sesión de administración, se registra un evento de esta categoría.
    - Advertencia: indica que se ha detectado un hecho inusual durante una operación, pero que no provocó que la operación fallara.
    - Error: indica el fallo de una operación debido a un error predecible.
    - Error Fatal: indica que ha ocurrido una circunstancia excepcional durante una operación.
- Fecha: Fecha y hora en la que ocurrió el evento.
- Autor: Nombre distintivo de la Autoridad que genero el evento.
- Rol: Tipo de Autoridad que generó el evento.
- Tipo de evento: Identifica el tipo del evento, distinguiendo, entre otro, los eventos
- criptográficos, de interface de usuario, de librería.
- Módulo: Identifica el módulo que generó el evento. Los posibles módulos son:
    - AC
    - AR

- Repositorio de información.
- Librerías de control de almacenamiento de información.

- Descripción: Representación textual del evento.

5.4.2. Frecuencia de procesado de Logs de auditoría

Se revisarán los logs de auditoría de forma periódica y en todo caso cuando se produce una alerta del sistema motivada por la existencia de algún incidente, en busca de actividad sospechosa o no habitual.

5.4.3. Periodos de retención para los Logs de auditoría

Se almacenará la información de los Logs de auditoría al menos durante 15 años.

5.4.4. Protección de los Logs de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante técnicas criptográficas, de forma que nadie, salvo las aplicaciones de visualización, con su debido control de accesos, pueda acceder a ellos.

Los dispositivos son manejados en todo momento por personal autorizado.

5.4.5. Procedimientos de backup de los Logs de auditoría

La AC dispone de un procedimiento adecuado de backup, de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de backup de los logs.

La AC tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando una copia de todos los logs de forma diaria.

5.4.6. Sistema de recogida de información de auditoria

La información de la auditoría de eventos es recogida internamente y de forma automatizada por el sistema operativo y por el software de certificación.

5.4.7. Notificación al sujeto causa del evento

No estipulado.

5.4.8. Análisis de vulnerabilidades

La AC realizará escaneos de vulnerabilidades periódicos sobre sus sistemas, registrará las pruebas y elaborará informes de los resultados obtenidos.

5.5. Archivo de registros

5.5.1. Tipo de eventos registrados

Se conservarán los eventos que tengan lugar durante el ciclo de vida del certificado, incluyendo la renovación del mismo. Se almacenará por la AC o, por delegación de ésta en la AR:

- Los especificados en el punto 5.4.1
- Las prácticas y políticas de certificación
- Todos los datos de la auditoría
- Todos los datos relativos a los certificados, incluyendo los contratos con los suscriptores y los datos relativos a su identificación
- Solicitudes de emisión y revocación de certificados
- Todos los certificados emitidos o publicados
- CRL's emitidas, respuestas de los métodos de validación online o registros del estado de los certificados generados
- La documentación requerida por los auditores

La AC es responsable del correcto archivo de todo este material y documentación.

5.5.2. Periodo de retención para el archivo

Todos los datos del sistema relativos al ciclo de vida de los certificados se conservarán durante el periodo que establezca la legislación vigente cuando sea aplicable. Los certificados se conservarán publicados en el repositorio durante al menos un año desde su expiración.

Los contratos con los suscriptores y cualquier información relativa a la identificación y autenticación del suscriptor serán conservados durante al menos 15 años o el periodo que establezca la legislación vigente.

Asimismo, la AC registrará y mantendrá accesible durante un período de tiempo apropiado, incluso cuando hayan cesado las actividades del prestador cualificado de servicios de confianza, toda la información pertinente referente a los datos expedidos y recibidos por el prestador cualificado de servicios de confianza, en particular al objeto de que sirvan de prueba en los procedimientos legales y para garantizar la continuidad del servicio. Esta actividad de registro podrá realizarse por medios electrónicos.

5.5.3. Protección del archivo

La AC asegura la correcta protección de los archivos mediante técnicas criptográficas, de forma que nadie, salvo las aplicaciones de visualización , con su debido control de accesos, pueda acceder a ellos.

La AC dispone de documentos técnica y de configuración donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

5.5.4. Procedimientos de backup del archivo

La copia de respaldo de los archivos se efectúa según las instrucciones técnicas y procedimiento de copia de seguridad establecidos por la AC cumpliendo lo definido en esta CPS.

5.5.5. Requerimientos para el sellado de tiempo de los registros

Se dispone de un servidor de tiempo basado en el protocolo NTP para mantener sincronizados los diferentes elementos que componen los sistemas fiables de certificación.

La fuente de sincronización del servidor de AC basada en el protocolo NTP (Network Time Protocol), es el Real Instituto y Observatorio de la Armada.

La sincronización de los servidores se lleva a cabo, al menos, una vez cada 24 horas

5.5.6. Sistema de recogida de registros

No estipulado.

5.5.7. Procedimientos para obtener y verificar información archivada

Durante la auditoria requerida por esta Declaración de Prácticas de Certificación (CPS), el auditor verificará la integridad de la información archivada.

El acceso a la información archivada se realiza solo por personal autorizado.

La AC proporcionará la información y los medios al auditor para poder verificar la información archivada.

5.6. Cambio de clave de una AC

En caso de cambio de claves de una CA , la nueva clave publica se distribuirá mediante la publicación de la misma en el repositorio que la AC dispone para tal efecto, en los repositorios indicados en el apartado 2.1.

5.7. Recuperación en caso de compromiso de la clave o desastre

5.7.1. Procedimientos de recuperación y gestión de incidentes

La AC ha desarrollado un plan de contingencias y procedimiento de gestión de incidentes para recuperar todos los sistemas en un máximo de cinco días, aunque se asegura la revocación y publicación de información del estado de los certificados en menos de 24 horas.

Cualquier fallo en la consecución de las metas marcadas por este plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

5.7.2. Corrupción de recursos, aplicaciones o datos

Según estipulado en punto 5.7.1 Procedimiento de recuperación y gestión de incidentes.

5.7.3. La clave de una entidad se compromete

El plan de contingencias de la AC trata el compromiso de la clave privada de CA como un desastre.

En caso de compromiso de la clave de CA, la AC al menos:

- Informará a todos los suscriptores, usuarios y otras CA's con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la AC www.acabogacia.org
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.
- Sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento del incidente de seguridad, notificará al organismo de supervisión y, en caso pertinente, a los fabricantes de software y a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.
- Si la CA Raíz estuviese comprometida, se revocarán todas las Cas Subordinadas y la CA Raíz y se generará una última ARL que se publicará en la web www.acabogacia.org junto con su Hash.
- En el caso de que el compromiso afecte a una CA subordinada:
    - Se revocará los certificados emitidos por la CA subordinada afectada.
    - Se revocará el certificado de la CA Subordinada y emitirá un ARL incluyendo el certificado de la CA comprometida.
    - Se publicará en la web de la AC www.acabogacia.org la última CRL con todos los certificados revocados y su HASH
    - Se publicará en la web de la AC www.acabogacia.org la ARL y su HASH.

5.7.4. Continuación de negocio después de un desastre

La AC reestablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con esta Declaración de Prácticas de Certificación (CPS) dentro de las 24 horas posteriores a un desastre o emergencia imprevista tomando como base el plan de contingencias y continuidad de negocio existente.

5.8. Cese del servicio

Antes del cese de su actividad la AC realizará las siguientes actuaciones:

- Informar al organismo de supervisión de cualquier cambio en la prestación de servicios de confianza cualificados, y de su intención de cesar tales actividades;

- Llevar a cabo su plan de cese para garantizar la continuidad del servicio conforme al Reglamento 910/2014 (eIDAs).
- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación hasta el cese definitivo de la actividad, si es el caso.
- Informará a todos los suscriptores, solicitantes, usuarios, otras CA's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente. Esta información será disponible a otros terceros de confianza a través de los canales oficiales de comunicación y como mínimo a través de la página web del Consejo General de la Abogacía Española
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- De acuerdo con el artículo 9.3c de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, la AC podrá transferir, con el consentimiento expreso de los suscriptores, la gestión de los certificados que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La AC informará, cuando sea el caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quién.
- En el caso de no transferir la gestión se revocarán los certificados en vigor en la fecha prevista de cese de servicio y los certificados de las CA Raíz y Subordinada y se publicarán las correspondientes CRLs y ARL.
- Con carácter previo al cese definitivo de la actividad, comunicará a la administración competente la información relativa a los certificados reconocidos expedidos al público cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el ReIDAS y el artículo 9.3c de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.,

6. Controles de Seguridad Técnica

La Autoridad de Certificación de la Abogacía usa hardware, software y procesos fiables, para conformar un sistema que garantiza la integridad, confidencialidad, y disponibilidad de la información y de los procesos de certificación.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

La generación de la clave de las CA's se realiza, de acuerdo con el proceso documentado de ceremonia de claves, dentro de la sala criptográfica del PSC, por personal adecuado según los roles de confianza y, al menos con un control dual y testigos de la organización titular de la AC y del auditor externo.

La generación de la clave de las CA's delegadas se realiza en un dispositivo que cumple los requisitos de seguridad necesarios.

Las claves son generadas usando el algoritmo de clave pública RSA y adicionalmente ECDSA para la jerarquía de ACA ROOT 2.

Las claves de las CA's tienen una longitud mínima de 4096 bits y 256 bits para la jerarquía de ACA ROOT 2.

Para las claves finales de los suscriptores consultar la política de certificación.

6.1.2. Entrega de la clave privada al suscriptor

Según lo dispuesto en cada Política de Certificación.

6.1.3. Entrega de la clave pública al emisor del certificado

El envío de la clave pública a la AC para la generación del certificado se realiza mediante un formato estándar preferiblemente en formato PKCS#10 o X509 autofirmado, utilizando un canal seguro para la transmisión.

6.1.4. Entrega de la clave pública de CA a los Usuarios

El certificado de las CA's de la cadena de certificación y su fingerprint (huella digital) estarán a disposición de los usuarios en http://www.acabogacia.org.

6.1.5. Tamaño de las claves

ACA emplea claves basadas en el algoritmo RSA con una longitud de 4096 bits en los certificados de CA.

Además, ACA emplea claves basadas en el algoritmo RSA de mínimo 2048 bits, ECC P-256 y ECC P-521 con una longitud de mínima de 256 bits en los certificados de CA de la jerarquía ACA ROOT 2.

6.1.6. Parámetros de generación de la clave pública

Las claves públicas de la CA Raíz, Cas Subordinadas y certificados de los firmantes, están codificadas de acuerdo con RFC 5280 y PKCS#1. El algoritmo de generación de claves es RSA y ECC para las CA's de la jerarquía ACA ROOT 2.

La verificación de calidad en ambos casos se realiza de acuerdo con la especificación técnica ETSI TS 102 176. Los algoritmos y parámetros de firma utilizados por las Cas y los certificados de firma son los siguientes.

- Algoritmo de Firma RSA
- Tamaño de claves = mínimo 4.096
- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-256

Para la jerarquía ACA ROOT 2, son los siguientes:

- Algoritmo de Firma: ECDSA
- Tamaño de claves = 256 y 512 bits
- Algoritmo de generación de claves: sha2-with-ecdsa
- Funciones criptográficas de Resumen:SHA-256 y SHA-512

6.1.7. Fines del uso de la clave

Los certificados incluyen la extensión Key Usage y Extended Key Usage, indicando los usos habilitados de la Claves.

6.2. Protección de la clave privada y controles de los módulos criptográficos

6.2.1. Estándares y controles de los módulos criptográficos

Los módulos criptográficos empleados en la CA emisora a entidades finales son homologados FIPS-140-2 nivel 3 y/o CCEAL4+

Almacén del dispositivo criptográfico:

A fin de prevenir la manipulación no autorizada del módulo criptográfico este está ubicado en un lugar seguro, con las siguientes características:

- Existe un inventario con el control de manipulación, entrada y salida del dispositivo

- El acceso al dispositivo está limitado a personal confiable.
- Todos los accesos fallidos quedan registrados en un log del sistema que gestiona el dispositivo
- Existen un procedimiento de gestión de incidentes y eventos anormales en el uso del dispositivo procediéndose a una investigación posterior y la emisión de reporte de la incidencia.
- El correcto funcionamiento del hardware se comprueba mediante los procedimientos de test ofrecidos por el fabricante al menos semanalmente.
- La manipulación del dispositivo criptográfico se realiza en presencia de al menos dos empleados confiables
- El dispositivo criptográfico está protegido con mecanismos de detección de manipulación.

Instalación del dispositivo criptográfico:

La instalación del dispositivo criptográfico se realiza en presencia de al menos dos empleados confiables.

Reparación del dispositivo criptográfico:

El dispositivo criptográfico será reparado en las condiciones que marcan los contratos de mantenimiento en vigor con el proveedor original del dispositivo. Se ejecutaran los procedimientos de test y control de funcionamiento iniciales una vez el dispositivo este recuperado.

Un dispositivo en un entorno de test nunca será utilizado en un entorno de producción a no ser que este quede inicializado de tal forma que su estado sea idéntico al que se tendría en el caso de que se recibiera nuevo.

Retirada de un dispositivo criptográfico:

La retirada del dispositivo criptográfico se realiza en presencia de al menos dos empleados confiables.

Si el dispositivo va a ser retirado de forma permanente los mecanismos de control de manipulación serán destruidos. El dispositivo se almacenara en un lugar protegido hasta su destrucción.

Reutilización de un dispositivo criptográfico:

Un dispositivo criptográfico podrá ser reutilizado siempre que se asegure que queda inicializado de tal forma que su estado sea idéntico al que se tendría en el caso de que se recibiera nuevo.

6.2.2. Control por más de una persona (m de n) sobre la clave privada´

El acceso y activación de las claves privadas de las CA's requiere el concurso simultáneo de dos dispositivos criptográficos controlados por personas diferentes de las distintas posibles, protegidos por una clave de acceso. Adicionalmente, el acceso físico a los dispositivos requiere la presencia de una tercera persona.

Se requiere de la presencia de un mínimo de tres personas con los roles específicos para poder acceder a la misma, siendo estos roles tanto de controles físicos como controles lógicos.

Las claves privadas generadas para los certificados de los usuarios finales se encuentran, bajo el exclusivo control de los firmantes, no estando estipulado que exista control multi-persona.

6.2.3. Custodia de la clave privada

Las claves privadas tanto de la AC raíz como de las AC subordinadas, se encuentran protegidas en el HSM y no son exportables.

En el ámbito de los certificados cualificados en QSCD en tarjeta, la AC no almacenará la clave privada del suscriptor en el modo llamado de key escrow.

Para las claves generadas en software, el usuario final es el encargado de su custodia, y éste será el responsable de mantenerla bajo su exclusivo control.

6.2.4. Backup de la clave privada

Existe un back up que permite la recuperación de las claves de la CA en caso de destrucción o inutilización del HSM, éste es recuperado sólo por el personal autorizado según los roles de confianza, usando, al menos un control de tres personas de confianza.

Las copias de backup de la clave privada de firma de la CA están almacenadas de forma segura. Este procedimiento se describe en detalle en la documentación de seguridad de la AC.

6.2.5. Archivo de la clave privada

La CA no archivará la clave privada de Firma de Certificados y CRLs después de la expiración del periodo de validez de la misma.

En el caso de las claves generadas en software de los certificados cualificados en software, el usuario final también es el encargado de su archivado, y responsable de mantenerla bajo su exclusivo control.

6.2.6. Transferencia de la clave privada en o desde el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos según se protocola en el documento de generación de claves requiriendo de la intervención de varias personas con diferentes roles y siguiendo las especificaciones del fabricante.

Se puede transferir la clave privada entre mismo tipo de módulo criptográfico siguiendo las instrucciones del fabricante.

6.2.7. Almacenamiento de la clave privada en modulo criptográfico.

Según especificaciones del fabricante.

6.2.8. Método de activación de la clave privada

Las claves de la CA se activan por un proceso de m de n.

Tal y como se estipula en el apartado 6.2.2 Control multi-persona de la clave privada, la clave privada tanto de la AC raíz como de la AC subordinada, se activa mediante la inicialización del software de AC por medio de la personación mínima de tres personas con roles específicos. Este es el único método de activación de dicha clave privada.

La activación de la clave privada del suscriptor se realiza mediante la introducción de al menos una contraseña tan sólo conocida por el titular y no almacenada en los sistemas, requiriendo de la utilización de los programas o sistemas informáticos que sirvan para aplicar los datos de creación de firma.

El acceso a la clave privada del suscriptor depende del dispositivo en el que esté generada, debiendo introducir al menos una contraseña tan sólo conocida por el titular y no almacenada en los sistemas.

La clave privada del suscriptor generada en QSCD en tarjeta, se activa mediante la introducción del PIN en el dispositivo seguro de creación de firma.

La clave privada del suscriptor generada en un dispositivo cualificado de creación de firmas electrónicas, se mantendrá y será controlada y gestionada por el suscriptor. Tendrá un sistema de protección contra intentos de acceso que bloqueen el dispositivo cuando se introduzca sucesivas veces un código de acceso erróneo.

6.2.9. Método de desactivación de la clave privada

Según lo dispuesto en las Políticas de Certificación.

6.2.10. Método de destrucción de la clave privada

Las claves privadas de la CA se destruirán de modo según los procedimientos habilitados por el HSM, para este propósito.

Previo a la destrucción, siempre debe revocarse el certificado asociado a la clave, si éste estuviese todavía vigente.

La destrucción de la clave privada del suscriptor consiste en el borrado de la clave privada y el certificado asociado al usuario del dispositivo cualificado de creación de firma.

En el ámbito de las claves generadas en software, la destrucción es también responsabilidad del suscriptor.

6.2.11. Evaluación del módulo criptográfico

Los dispositivos criptográficos utilizados por las autoridades de certificación cumplen con los requisitos de seguridad necesarios para garantizar la protección de las claves de las Autoridades de Certificación.

Dichos dispositivos son resistentes a manipulaciones intrusivas a nivel hardware (tamper protection).

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

La AC conservará todas las claves públicas durante el periodo exigido por la legislación vigente, cuando sea aplicable, o mientras el servicio de certificación este activo y 6 meses más como mínimo, en otro caso.

6.3.2. Periodo de uso para las claves públicas y privadas

El periodo de uso de un certificado será determinado por la validez temporal del mismo.

La caducidad producirá automáticamente la invalidación de los Certificados, originando el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de confianza. Si no se produce un cese de la actividad del TSP, previa a la caducidad del certificado de la AC, se generará una nueva AC (nuevo par de claves) en las mismas condiciones de seguridad que la que está a punto de expirar, y se notificará a todas las partes la existencia de la nueva AC. El certificado de la nueva AC se publicará y distribuirá tal y como se especifica para el actual en esta DPC.

Todo este proceso de generación de la nueva AC se hará con la suficiente antelación y previsión con el fin de minimizar el impacto en terceros.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

El dispositivo cualificado de creación de firmas electrónicas utiliza una clave de activación para el acceso a las claves privadas. La clave de activación también es requerida para aquellas claves generadas en software.

Los dispositivos seguros de creación de firma (tarjeta) llevan incorporado de fábrica un sistema de activación de clave mediante PIN de transporte que debe ser modificado por el suscriptor en el momento de la entrega física de la tarjeta.

6.4.2. Protección de datos de activación

En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se entregarán mediante un proceso que asegure la confidencialidad de los mismos ante terceros. En ningún caso, las ARs custodiaran los datos de activación del dispositivo cualificado de creación de firmas electrónicas.

El suscriptor es el responsable de la protección de los datos de activación de su clave privada. AC Abogacía requiere una contraseña o PIN para el acceso a la clave privada, también requerida para el proceso de firma y un segundo factor de autenticación en el caso de certificados en QSCD.

Cuando la generación se realiza en software, la instalación y activación de la clave privada asociada a los certificados, requiere la utilización de los sistemas de seguridad del propio usuario, debiendo introducir como mínimo una contraseña tan sólo conocida por él y no almacenada en los sistemas.

6.4.3. Otros aspectos de los datos de activación

Sin especificar

6.5. Controles de seguridad informática

La AC utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad y la fiabilidad técnicas de los procesos que sustentan.

Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas en los siguientes aspectos:

Configuración de seguridad del sistema operativo.

Configuración de seguridad de las aplicaciones.

Dimensionamiento correcto del sistema.

Configuración de Usuarios y permisos.

Configuración de eventos de log.

Plan de backup y recuperación.

Requerimientos de tráfico de red.

La documentación técnica y de configuración de la AC detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.5.1. Requerimientos técnicos de seguridad informática específicos

Cada servidor de la AC incluye las siguientes funcionalidades:

- ✓ control de acceso a los servicios de AC y gestión de privilegios.
- ✓ imposición de separación de tareas para la gestión de privilegios.
- ✓ identificación y autenticación de roles asociados a identidades.
- ✓ archivo del historial del suscriptor y la AC y datos de auditoría.
- ✓ auditoria de eventos relativos a la seguridad.
- ✓ auto-diagnóstico de seguridad relacionado con los servicios de la AC.
- ✓ Mecanismos de recuperación de claves y del sistema de AC.

Las funcionalidades expuestas son provistas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.

6.5.2. Valoración de la seguridad informática

La seguridad de los equipos viene reflejada por un análisis de riesgos iniciales de tal forma que las medidas de seguridad implantadas son respuesta a la probabilidad e impacto producido cuando un grupo de amenazas definidas puedan aprovechar brechas de seguridad.

Los productos utilizados para la prestación de servicios de certificación disponen de certificación Common Criteria y/o FIPS 140-2.

La seguridad física está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal.

6.6. Controles de seguridad del ciclo de vida

6.6.1. Controles de desarrollo del sistema

La AC posee un procedimiento de control de cambios en las versiones de sistemas operativos y aplicaciones que impliquen una mejora en sus funciones de seguridad o que corrijan cualquier vulnerabilidad detectada.

6.6.2. Controles de gestión de la seguridad

Se utiliza una metodología formal de gestión de configuración para la instalación y el mantenimiento continuo de los sistemas de ACA sobre la base de la norma UNE-ISO/IEC 27001:2014 y ISO/IEC 27001:2017

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

AC Abogacía evalúa el nivel de seguridad a través de Auditorías.

6.6.4. Controles del ciclo de vida de los dispositivos seguros de creación de Firma

ACA realiza las revisiones oportunas para verificar el estado de validez de la certificación de los dispositivos seguros de creación de Firma.

La fuente de consulta es la siguiente: https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd

6.7. Controles de seguridad de la red

La AC protege el acceso físico a los dispositivos de gestión de red y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras se realiza de forma encriptada.

6.8. Sellado de tiempo

No estipulado

7. Perfiles de Certificado y CRL y OCSP

7.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3, la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", ETSI TS 101 862 conocida como"European profile for Qualified Certificates" y las RFC 3039 (substituída) y 3739 "Qualified Certificates Profile". También se ha tenido en cuenta la familia 319 412 en relación a los perfiles de los certificados. El tamaño de los campos puede ser superior a los establecidos en la RFC 5280.

El contenido de los certificados cualificados es conforme con el artículo 28 del Reglamento 910/2014 (ReIDAS).

Aclaraciones sobre la extensión "x509v3 KeyUsage" (uso de las claves):

La RFC 5280 que define los perfiles de los certificados X509 sustituye por obsolescencia a la RFC 2459 y la RFC 3280. Un cambio importante es que el uso de la clave "digital signature" como se define en la RFC 5280 no declara dicho uso como aquel adecuado a firmas digitales para servicios de seguridad diferentes del "no repudio", tal como expresaba la cláusula correspondiente en la RFC 2459.

Coherentemente con la antigua RFC 2459, la RFC 3039 obligaba a que si el uso definido como "no repudio" estaba presente, lo hiciera de manera exclusiva frente a cualquier otro uso. El cambio citado anteriormente generó una petición a la ITU para corregir el error y armonizar la RFC 3039 respecto a las actualizadas RFC 3280 y posteriormente RFC 5280.

La RFC 3739 "Qualified Certificates Profile" (Marzo 2004, substituye a la RFC 3039) no se manifiesta en el apartado correspondiente sobre el uso "no repudio", remitiéndose a las políticas del PSC o a requerimientos legales específicos aplicables al ámbito de emisión, y haciendo una consideración sobre los posibles riesgos de combinar el uso "no repudio" con otros.

Por otra parte, la funcionalidad de no repudio, se consigue por la aplicación del mecanismo de firma digital a los datos objeto de firma, y por la existencia de un servicio o aplicación de no repudio. Este servicio requerirá la existencia del Key Usage "no repudio" en el certificado del firmante, así como la aplicación de mecanismos adicionales (como pueden ser los sellos de tiempo emitidos por una Autoridad de Sellado de Tiempos, validación por OCSP, etc), según los propios estándares técnicos.

Los certificados tendrán el contenido y campos descritos según lo dispuesto en cada Política de Certificación. Los datos relativos a los certificados de las CA Root y CAs Subordinadas, se encuentran en el apartado 1.3.1 Autoridad de Certificación

7.1.1. Número de versión

La AC emite certificados X.509 Versión 3.

7.1.2. Extensiones del certificado

Según lo dispuesto en cada Política de Certificación.

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1. 2. 840. 113549. 1. 1. 11 SHA-256 with RSA Encryption
- 1.2.840.10045.4.3.2 ecdsaWithSHA256 (Certificados finales de la jerarquía ACA ROOT 2)
- 1.2.840.10045.4.3.4 ecdsaWithSHA512 (Certificados de OCSP)
- 1.2.840.10045.4.3.4 ecdsaWithSHA512 (CA's de la jerarquía ACA ROOT 2)

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption
- 1.3.132.0.35 secp521r1 (CA's y OCSP de la jerarquía ACA ROOT 2)

7.1.4. Formato de los nombres

Los certificados contienen el "distinguished name X.500" del emisor y del suscriptor del certificado en los campos "issuer" y "subject" respectivamente.

7.1.5. Restricciones de los nombres

Según lo dispuesto en cada Política de Certificación.

7.1.6. Identificador de objeto de política de certificado

Según lo dispuesto en cada Política de Certificación.

7.1.7. Empleo de la extensión restricciones de política

La extensión "Policy Constrains" del Certificado raíz de la AC no está definida.

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión "Certificate Policies" incluye.

- Policy que contiene el OID de la política
- CPS que contiene una URL al repositorio de políticas y CPS

Además, para ACA ROOT 2, según lo dispuesto en cada Política de Certificación.

7.1.9. Tratamiento semántico para la extensión “Certificate policy”

La extensión “Certificate Policy” incluye el campo OID de política, que identifica la política asociada al Certificado por parte de ACA

7.2. Perfil de CRL

El perfil de las CRL’s se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 versión 3 de la RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". Las CRL’s son firmadas por la autoridad de certificación que ha emitido los certificados.

7.2.1. Número de versión

Las CRL emitidas por la AC son conformes al estándar X.509 versión 2.

7.2.2. CRL y extensiones

Según lo dispuesto en cada Política de Certificación.

7.3. Perfil de OCSP

El perfil del certificado de OCSP se corresponde con el propuesto en las políticas de certificación correspondientes, y con el estándar X.509 versión 3 de la RFC 6960 "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".

7.3.1. Número de versión

Los certificados de OCSP Responder utilizarán el estándar X.509 versión 3 (X.509 v3).

7.3.2. OCSP y extensiones

En la jerarquía ACA ROOT, las extensiones para OCSP empleadas en el perfil del certificado son:

- Key Usage, marcado como obligatorio y crítico.
- Enhanced Key usage, marcado únicamente como obligatorio.

En la jerarquía ACA ROOT 2, las extensiones para OCSP empleadas en el perfil del certificado son:

- Issuer Alternative Name
- Authority/Subject key Identifier
- Key Usage, marcado como obligatorio y crítico.
- Enhanced Key usage, marcado únicamente como obligatorio.
- NoCheck

8. Auditorias de conformidad

8.1. Frecuencia de las auditorías

Se realiza una auditoria con carácter periódico. Por otro lado, el prestador de servicios de certificación/ prestador cualificado de servicios de confianza será auditado, al menos cada 24 meses en cumplimiento del Reglamento 910/2014.

Sin perjuicio de lo anterior, el prestador realizará auditorías internas bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.2. Identificación y calificación del auditor

Las auditorías en cumplimiento del Reglamento 910/2014 son realizadas por un organismo de evaluación de la conformidad y sus auditores deben cumplir con los requisitos indicados en la norma europea ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI);

Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

Asimismo, se podrán llevar a cabo auditorías Webtrust realizadas por una firma de auditoría de primer nivel, según criterios WebTrust for Certification Authorities, que se pueden descargar y consultar en http://www.aicpa.org, desarrollados por la AICPA (American Institute of Certified Public Accountants, Inc.) y la CICA (Canadian Institute of Chartered Accountants).

Los Principios y Criterios WebTrust para CA son consistentes con los estándares desarrollados por la American National Standards Institute (ANSI) y la Internet Engineering Task Force (IETF)

8.3. Relación entre el auditor y la AC

El auditor será una conocida empresa con departamentos especializados en auditoria informática de reconocido prestigio sin existir ningún conflicto de intereses que pueda desvirtuar su actuación en su relación con AC Abogacía.

8.4. Tópicos cubiertos por la auditoria

La auditoría verifica los siguientes principios:

- Publicación de la Información: Que la AC hace públicas las Prácticas de Negocio y de Gestión de Certificados (Políticas y Declaración de Prácticas de Certificación (CPS)), así como la protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.
- Integridad de Servicio. Que la AC mantiene controles efectivos para asegurar razonablemente que:
    - La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la AC).

- La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.

- Controles generales. Que la AC mantiene controles efectivos para asegurar razonablemente que:
  - La información de suscriptores y usuarios está restringida a personal autorizado y protegida de usos no especificados en las prácticas de negocio de la AC publicadas.
  - Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.
  - Las tareas de explotación, desarrollo y mantenimiento de los sistemas de la AC son adecuadamente autorizadas y realizadas para mantener la integridad de los mismos.
- Así como los criterios de auditoría enumerados en la norma europea ETSI EN 319 403 Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.

Auditoría en las Autoridades de Registro. Todas las Autoridades de Registro podrán ser auditadas previamente a su puesta en marcha efectiva. Adicionalmente, se podrán realizan auditorias periódicas que comprueban el cumplimiento de los requerimientos exigidos por las políticas de certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

8.5. Resolución de incidencias

En caso de que sean detectadas incidencias o no-conformidades, se habilitarán las medidas oportunas para su resolución en el menor tiempo posible.

8.6. Comunicación de resultados

En cualquier caso, el prestador cualificado de servicios de confianza, sin demoras indebidas pero en cualquier caso en un plazo de 24 horas tras tener conocimiento de los incidentes de seguridad, notificarán al organismo de supervisión y, en caso pertinente, a otros organismo relevantes como el organismo nacional competente en materia de seguridad de la información, o la autoridad de protección de datos, cualquier violación de la seguridad o pérdida de la integridad que tenga un impacto significativo en el servicio de confianza prestado o en los datos personales correspondientes.

Cuando la violación de seguridad o la pérdida de integridad puedan atentar contra una persona física o jurídica a la que se ha prestado el servicio de confianza, el prestador de servicios de confianza notificará también a la persona física o jurídica, sin demora indebida, la violación de seguridad o la pérdida de integridad.

9. Otros temas legales y Operativos

9.1. Tarifas

9.1.1. Tarifas de emisión de certificados y renovación

Los precios de los servicios de certificación o cualquier otro servicio relacionado estarán disponibles para los usuarios en las diferentes Autoridades de Registro.

9.1.2. Tarifas de acceso a los certificados

El acceso a los certificados emitidos será gratuito, no obstante, la AC podrá imponer alguna tarifa para los casos de descarga masiva de certificados o cualquier otra circunstancia que a juicio de la AC deba ser gravada, en cuyo caso se publicarán dichas tarifas en la página web de la AC.

9.1.3. Tarifas de acceso a la información relativa al estado de los certificados o los certificados revocados

La AC proporcionará a cualquier parte usuaria información sobre el estado de validez o revocación de los certificados cualificados expedidos por ellos. Esta información se encuentra disponible al menos por cada certificado en cualquier momento y con posterioridad al período de validez del certificado en una forma automatizada que es fiable, gratuita y eficiente.

9.1.4. Tarifas por otros servicios

Las tarifas aplicables a otros servicios se publicarán en la página web de la AC.

9.1.5. Política de reintegros

Sin estipulación.

9.2. Responsabilidad financiera

La AC, en su actividad como prestador cualificado de servicios de confianza mantiene recursos económicos suficientes para afrontar el riesgo de la responsabilidad por daños y perjuicios ante los usuarios de sus servicios y a terceros, garantizando sus responsabilidades en su actividad de Prestador tal como se establece la legislación aplicable.

9.2.1. Cobertura del seguro

En concreto, la garantía citada en el anterior apartado se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a 3.000.000 €.

9.2.2. Otros activos

No estipulado

9.2.3. Cobertura del seguro o garantía para entidades finales

No estipulado

9.3. Confidencialidad de la información de negocio

El Consejo General de la Abogacía Española es Responsable del tratamiento de los datos de la Autoridad de Certificación de la Abogacia (la AC), y cumple con la normativa de protección de datos de forma específica con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante el Reglamento General de Protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante la LOPD-GDD),

La AC dispone de una adecuada política de tratamiento de la información y de los modelos de acuerdo que deberán firmar todas las personas que tengan acceso a información confidencial.

9.3.1. Tipo de información a mantener confidencial

La AC considerará confidencial toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.3.2. Tipo de información considerada no confidencial

La siguiente información será considerada no confidencial:

- La contenida en la presente Política y en las Prácticas de Certificación.
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo de manera no exhaustiva
    - Los certificados emitidos o en trámite de emisión.
    - La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación/ Prestador cualificado de servicios de confianza.
    - El nombre, los apellidos y el número de documento nacional de identidad del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
    - La dirección de correo electrónico del suscriptor del certificado, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de colectivo, o la dirección de correo electrónico asignada por el suscriptor, en caso de certificados para dispositivos.

- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.

- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Cualquier información cuya publicidad sea impuesta normativamente.

9.3.3. Responsabilidad de proteger la información confidencial

ACA y sus Autoridades de Registros tendrán la obligación de proteger toda aquella información considerada confidencial

Los certificados serán objeto de publicación de acuerdo con lo establecido en el artículo 9.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

9.4. Protección de datos de carácter personal

9.4.1. Política de protección de datos de carácter personal

El Consejo General de la Abogacía Española es Responsable del tratamiento de los datos de la Autoridad de Certificación de la Abogacia (la AC), y cumple con la normativa de protección de datos de forma específica con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante el Reglamento General de Protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante la LOPD-GDD),

Identidad y datos de contacto del responsable del tratamiento de ACA

Consejo General de la Abogacía Española

Domicilio: Paseo de Recoletos, 13, 28004 – Madrid.

Teléfono de contacto: 915232593

Dirección electrónica: info@acabogacia.org

Datos de contacto del delegado de protección de datos

Paseo de Recoletos, 13. 28004- Madrid.

info@acabogacia.org

Los datos contenidos en el directorio de certificados que tengan la consideración de datos de carácter personal a efectos de lo dispuesto en el Reglamento General de Protección de datos.

9.4.2. Información personal tratada como privada

Se considerará información personal y se tratará como privada cualquier información de carácter personal que no esté contenida en el apartado siguiente.

9.4.3. Información personal tratada como pública

La siguiente información será considerada pública:

- La contenida en la presente Política y en las Prácticas de Certificación.
- La información contenida en los certificados, puesto que para su emisión el suscriptor otorga previamente su consentimiento, incluyendo de manera no exhaustiva:
    - Los certificados emitidos o en trámite de emisión.
    - La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación/ Prestador cualificado de servicios de confianza.
    - El nombre, los apellidos y el número de documento nacional de identidad del suscriptor del certificado, en caso de certificados individuales, así como cualquier otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
    - La dirección de correo electrónico del suscriptor del certificado, en caso de certificados individuales, o del poseedor de claves, en caso de certificados de colectivo, o la dirección de correo electrónico asignada por el suscriptor, en caso de certificados para dispositivos.
    - Los usos y límites económicos reseñados en el certificado.
    - El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
    - El número de serie del certificado.
    - Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRL's), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.

9.4.4. Responsabilidad de proteger la información privada

La AC considerará privada toda la información que no esté catalogada expresamente como pública. No se difunde información declarada como confidencial sin el consentimiento expreso por escrito de la entidad u organización que le haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

9.4.5. Notificación y consentimiento para utilizar los datos de carácter personal privados

Sin menoscabo de otras obligaciones, las Autoridades de Registro que se constituyan verificarán que el solicitante de un certificado presta su consentimiento al tratamiento de sus datos de carácter personal, previa información del Responsable del tratamiento de su legitimación, de la finalidad a la que se van a destinar, y los derechos que le asisten de acuerdo con el Artículo 13 del Reglamento General de Protección de datos.

En los casos en los que los datos no hayan sido recabados directamente de los interesados, la AC informará de forma expresa, precisa e inequívoca a estos, dentro de los tres meses siguientes al momento del registro de los datos, de lo indicado en el párrafo anterior.

9.4.6. Divulgación de la información por requerimiento judicial o administrativo

Se proporcionará la información solicitada por la autoridad competente en los casos y forma establecidos legalmente.

9.4.7. Otras circunstancias de divulgación de la información

Se proporcionara información solicitada cuando así lo permita la presente Declaración de Prácticas de Certificación (CPS) o las Políticas de Certificación de ACA.

9.5. Derechos de propiedad intelectual

La propiedad intelectual de esta Declaración de Prácticas de Certificación (CPS) pertenece al CGAE.

AC Abogacía será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita.

AC Abogacía concede licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de aplicación de esta política, según se define en la sección 1 y de acuerdo con el correspondiente instrumento vinculante entre el AC Abogacía y la parte que reproduzca y/o distribuya el certificado.

9.6. Responsabilidad y Garantías

El Consejo General de la Abogacía Española (CGAE), en su actividad de prestación cualificada de servicios de confianza, responderá por el incumplimiento de lo establecido en las Políticas y Prácticas de certificación y, allí donde sea aplicable, por lo que dispone el Reglamento n 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza

Asimismo, el Consejo General de la Abogacía Española asumirá toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.

Sin perjuicio de lo anterior el Consejo General de la Abogacía Española no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las Políticas y Prácticas de Certificación y en el ReIDAS la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y su normativa de desarrollo, donde sea aplicable.

9.6.1. Responsabilidad y garantías de la AC

La AC se obliga según lo dispuesto en los artículos 20 al 24 de ReIDAS y en el artículo 9 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en las demás normativas sobre prestación de servicios de certificación, así como lo dispuesto las Políticas de Certificación y en esta Declaración de Prácticas de Certificación (CPS). De forma específica la AC se le requiere a:

- No almacenar ni copiar los datos de creación de firma del Suscriptor, cuando así lo disponga la normativa vigente.
- Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá trasmitirse forma gratuita, por escrito o por vía electrónica:
    - Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento de revocación o suspensión de su certificado y los dispositivos de creación y de verificación de firma electrónica compatibles con el certificado expedido.
    - Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.
    - El método utilizado por la AC para comprobar la identidad del firmante u otros datos que figuren en el certificado.
    - Las condiciones precisas de utilización del certificado, sus límites de uso y la forma en que la AC garantiza su responsabilidad patrimonial.
    - Las certificaciones obtenidas por la AC.
    - Los procedimientos aplicables para las resoluciones judiciales o extrajudiciales.
    - O cualquier otra información contenida en la presente Declaración de Prácticas de Certificación (CPS) o en las Políticas de Certificación.
- Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida.
- Poner mecanismos razonables de seguridad para mantener la integridad del directorio de certificados
- Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro
- Suspender y revocar los certificados según lo dispuesto en la Declaración de Prácticas de Certificación (CPS) y publicar las mencionadas revocaciones en los sistemas de validación de certificados habilitados a tal efecto.
- Informar a los Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación española vigente.
- Publicar las Políticas y Prácticas de Certificación en la página web de la AC de forma gratuita.

- Informar sobre las modificaciones de esta Declaración de Prácticas de Certificación a los Subscriptores, AR's que estén vinculadas a ella y usuarios, mediante la publicación de estas y sus modificaciones en su página web.
- Garantizar que pueda determinarse la fecha y la hora en las que se expidió un certificado, se extinguió o suspendió su vigencia.
- Emplear personal con la cualificación, conocimientos experiencia necesarios para la prestación de los servicios de certificación ofrecidos por la AC.
- Utilizar sistemas fiables para almacenar certificados cualificados que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
- Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Notificar a suscriptores el cambio de estado de la certificación de los dispositivos seguros de creación de Firma.
- Tomar medidas contra la falsificación de certificados y garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.
- Disponer de un seguro de responsabilidad civil que debe cubrir un valor mínimo en la medida en que sea exigible por la normativa vigente
- Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente, cuando sea aplicable
- Emitir certificados conforme a estas Prácticas y a los estándares de aplicación.
- Proteger sus claves privadas de forma segura.
- Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
- Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente, cuando sea aplicable.
- Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase.
- Respetar lo dispuesto en las Políticas y Prácticas de Certificación.
- Cumplir con aquellos requisitos del art 24 (ReIDAS) no citados con anterioridad para los prestadores cualificados de servicios de confianza.

9.6.2. Responsabilidad y garantías de las AR

Las Autoridades de Registro son delegadas por la AC para realizar esta labor, por lo tanto la AR también se obliga en los términos definidos en las Prácticas de Certificación para la emisión de certificados, principalmente:

- Abonar las tarifas establecidas por los servicios de certificación solicitados.
- Respetar lo dispuesto en esta Declaración de Prácticas de Certificación (CPS).

- Comprobar la identidad de los suscriptores y solicitantes de certificados.
- Verificar la exactitud y autenticidad de la información suministrada por el solicitante.
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el suscriptor.
- Respetar lo dispuesto en los contratos firmados con la AC.
- Respetar lo dispuesto en los contratos firmados con el Suscriptor.
- Informar a la AC las causas de revocación, siempre y cuando tomen conocimiento.
- Que las ARs se comprometen a cumplir con los requerimientos generales de seguridad indicados por la AC.

9.6.3. Responsabilidad y garantías de los suscriptores

El Suscriptor de un Certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Custodiar su clave privada de manera diligente.
- Usar el certificado según lo establecido en la presente Declaración de Prácticas de Certificación (CPS) y las Políticas de Certificación aplicables.
- Respetar lo dispuesto en los documentos firmados con la AR.
- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.
- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la AC o la AR de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

9.6.4. Responsabilidad y garantías de los usuarios

Será obligación de los Usuarios cumplir con lo dispuesto por la normativa vigente y además:

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía.
- Comprobar por sus propios mecanismos, que la jerarquía con la que se encuentra emitido el certificado se encuentra en la lista de certificados cualificados de la unión europea (TSL).

9.6.5. Responsabilidad y garantías de otros participantes

El solicitante de un Certificado estará obligado a cumplir con lo dispuesto por la normativa vigente y además a:

- Suministrar a la AR la información necesaria para realizar una correcta identificación.
- Realizar los esfuerzos que razonablemente estén a su alcance para confirmar la exactitud y veracidad de la información suministrada.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

9.7. Exoneración de responsabilidad

La relación entre la AC y las AR se regirá por su especial relación contractual. La AC y las AR's se exonerarán de su responsabilidad en los términos establecidos en la Declaración de Prácticas de Certificación (CPS) y las políticas de certificación. En particular, la AC y las AR's no serán responsables en ningún caso cuando se encuentre ante cualquiera de estas circunstancias:

1. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente Declaración de Prácticas de Certificación (CPS), en particular por la utilización de un certificado suspendido o revocado, o por depositar la confianza en él sin verificar previamente el estado del mismo.
2. Por el uso indebido o fraudulento de los certificados o los sistemas de validación de certificados habilitados a tal efecto.
3. Por el uso indebido de la información contenida en el Certificado o en los sistemas de validación de certificados habilitados a tal efecto.
4. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Usuarios en la normativa vigente, la presente Declaración de Prácticas de Certificación (CPS) o en la Política de Certificación correspondiente.
5. Por el contenido de los mensajes o documentos firmados o cifrados digitalmente.
6. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.
7. Fraude en la documentación presentada por el solicitante.

9.8. Límite de responsabilidad

El Consejo General de la Abogacía Española, en su actividad de Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza responderá de acuerdo con el régimen de responsabilidad que establece establece ReIDAS, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza , en las demás normativas sobre prestación de servicios de certificación y el resto de la legislación aplicable.

La AC será responsable del daño causado ante el Suscriptor o cualquier persona que, de buena fe, confíe en el certificado, siempre que por parte de la propia AC exista dolo, culpa o negligencia, respecto de:

1. La exactitud de toda la información contenida en el certificado en la fecha de su emisión.
2. La garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el certificado.
3. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
4. La correspondencia entre el certificado solicitado y el certificado entregado

5. Cualquier responsabilidad que se establezca por la legislación vigente

9.9. Indemnizaciones

No estipulado

9.10. Periodo de validez de este documento

9.10.1. Plazo

La presente Declaración de Prácticas de Certificación (CPS) y las diferentes Políticas de Certificación entrarán en vigor en el momento de su publicación.

9.10.2. Terminación

La presente Declaración de Prácticas de Certificación (CPS) y las diferentes Políticas de Certificación serán derogadas en el momento que una nueva versión de cualquier documento sea publicado. La nueva versión sustituirá íntegramente al documento anterior. ACA se compromete a someter dicha Declaración a un proceso de revisión periódico

9.10.3. Efectos de la terminación

Para los certificados vigentes emitidos bajo una Declaración de Prácticas y Políticas de Certificación anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11.Notificaciones individuales y comunicación con los Usuarios

ACA establece en el instrumento jurídico vinculante con el suscriptor los medios y plazos para las notificaciones.

De modo general, se utilizará la página web de Abogacia, www.abogacia.es para realizar cualquier tipo de notificación y comunicación.

9.12.Modificaciones de este documento

Se realizarán modificaciones de esta Declaración de Prácticas de Certificación (CPS) cuando se produzca algún cambio relevante de carácter técnico, jurídico o procedimental en la actividad de la Autoridad de Certificación.

Adicionalmente, se realizará una revisión anual independiente de las revisiones realizadas por cambios.

Cualquier elemento de esta Declaración de Prácticas de Certificación (CPS) puede ser cambiado unilateralmente por AC Abogacía sin preaviso. Las modificaciones deben estar justificadas desde un punto de vista legal, técnico o comercial.

9.12.1. Procedimiento de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los usuarios de esta política serán notificados inmediatamente a los suscriptores mediante la publicación en la web de AC Abogacía, haciendo referencia expresa en la "página principal" de la misma a la existencia del cambio.

Los usuarios afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 15 días siguientes a la recepción de la notificación.

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la AC.

9.12.2. Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta política sin requerir de notificación son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

9.12.3. Circunstancias en las que se cambiará el OID

Se procederá al cambio de OID en aquellas circunstancias que se altere, de forma significativa, alguno de los procedimientos descritos en el presente documento.

Se procederá a cambiar el OID siempre que se considere que se está emitiendo un nuevo tipo de certificado.

9.13. Resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante un proceso de Mediación solicitado al Centro de Mediación del Colegio de Abogados o uno de arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral.

Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

9.14.Legislación aplicable

El presente documento especifica la Declaración de Prácticas de Certificación de la Autoridad de Certificación constituida por el Consejo General de la Abogacía Española, denominada Autoridad de Certificación de la Abogacía (AC Abogacía), para la emisión de certificados personales, y está basada en la especificación del estándar RCF 3647 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, de IETF.

Asimismo, para el desarrollo de su contenido, se ha tenido en cuenta estándares europeos, entre los que cabe destacar los siguientes:

- ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile.
- ETSI EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates.

- 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 319 411-1: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI EN 319 401: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Igualmente, se ha considerado como normativa básica aplicable a la materia:

- Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (en adelante ReIDAS) y por el que se deroga la Directiva 1999/93/CE.
- la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza , en las demás normativas sobre prestación de servicios de certificación
- Real Decreto-Legislativo 1/1996, de 12 de abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

9.15.Cumplimiento de la legislación aplicable

En cualquier caso, ACA manifiesta el cumplimiento de las normativas indicadas así como el cumplimiento estricto de la Declaración de Practicas de Certificación (CPS) así como de cada una de las Políticas de Certificación.

9.16.Otras disposiciones

Cada cláusula de esta Declaración de Prácticas de Certificación es válida en sí misma y no invalida al resto. La cláusula inválida o incompleta puede ser sustituida por otra equivalente.

Anexo 1: Documento de Seguridad

PREAMBULO

El Consejo de la Abogacía, es Responsable del tratamiento de los datos de la Autoridad de Certificación de la Abogacía (la AC) y cumple con la normativa de protección de datos de forma específica con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante el Reglamento General de Protección de datos) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante la LOPD-GDD).

El tratamiento de datos que realizad la Autoridad de Certificación de la Abogacía está recogido en el Registro de Actividades de Tratamiento de la Abogacia (RAT) que se encuentran en el Portal de Transparencia de la Abogacía y las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y que se encuentran descritas en los documentos que conforman la política de protección de datos y seguridad de la información del Consejo General de la Abogacía.

ACA cuenta con la certificación ENS por una entidad acreditada que estará disposición de los usuarios.

Los Usuarios (terceros que confían en los certificados) pueden consultar los datos contenidos en los certificados así como el estado de vigencia o validez en el directorio de certificados, de acceso público según lo establecido en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y en las demás normativas sobre prestación de servicios de certificación. Los Usuarios únicamente podrán utilizar la información para la verificación de la validez del certificado o de las firmas generadas de acuerdo con lo establecido en la legislación vigente, la Declaración de Prácticas de Certificación (CPS) y las Políticas de Certificación. Se advierte, con carácter general, que cualquier tratamiento, registro o utilización para otros fines distintos de los anteriores requiere obligatoriamente del consentimiento previo de los titulares de los datos.

Los Usuarios de un certificado ACA tiene derecho a obtener confirmación sobre si estamos tratando datos personales que te conciernen o no. Asimismo y en relación con sus datos personales tienes derecho a:

- Acceder a los mismos.
- Solicitar su rectificación o supresión.
- Solicitar la limitación de su tratamiento.
- Oponerse a su tratamiento.
- Solicitar su portabilidad en un formato estructurado, de uso común y de lectura mecánica.

Podrá ejercer tales derechos ante el Consejo General de la Abogacía Española. Para ello deberá dirigirse por escrito al Consejo en la dirección indicada, acompañando a tu solicitud una copia de documento de identificación, o enviando un correo electrónico que incluya firma electrónica, con el objeto de acreditar tu identidad, a informacion@abogacia.es.

AMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento, parte integrante de la Declaración de Prácticas de Certificación (CPS) de AC Abogacía, tiene como finalidad establecer las medidas técnicas y organizativas necesarias para garantizar

la seguridad que deben reunir los ficheros automatizados, locales, equipos, sistemas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

En la Declaración de Prácticas de Certificación (CPS) se detallan las medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el Reglamento antes mencionado, al objeto de garantizar la seguridad de los datos de carácter personal de la cual es responsable esta institución.

Adicionalmente, se establecen las medidas generales de seguridad aplicables a cualquier sistema de información en uso en el Consejo General de la Abogacía Española, aunque dicho sistema no esté incluido entre los que soportan directamente la prestación de los servicios de certificación.

La Declaración de Prácticas de Certificación (CPS), de la cual forma parte este Documento de Seguridad es de obligado cumplimiento para todo el personal de la institución incluido en el apartado 5.2.1.

TIPO DE DATOS DE CARÁCTER PERSONAL QUE UTILIZA LA AUTORIDAD DE CERTIFICAICÓN

Los datos personales que constituyen que son objeto de tratamiento son los siguientes:

Datos de Identificación:

- Nombre, Apellidos y NIF

Datos de contacto:

- Dirección de correo electrónico
- Dirección de correo electrónico alternativa para contacto

Datos profesionales:

- Colegio o Institución
- Nº de Colegiado / Asociado (donde sea aplicable)
- Status respecto de la corporación / entidad (donde sea aplicable)
- Cargo, Título o especialidad (donde sea aplicable)
- Departamento al que pertenece (donde sea aplicable)

Datos del certificado de clave digital de clave pública:

- Nº de serie del certificado
- Fecha de inicio y fin de validez
- Clave pública asociada a la clave privada en poder del usuario
- Estado de la petición y del certificado (Pendiente de aprobar, Aprobado, Válido, Suspendido, Revocado).

<u>Descripción del sistema de tratamiento</u>

- El sistema que da soporte a la prestación de servicios de certificación se basa en servidores centralizados ubicados en un CPD de alta seguridad. El sistema tiene acceso local a través de estaciones de trabajo controladas ubicadas en la zona segura del CPD, y a través de Internet.
- Las operaciones de consulta del sistema de publicación de certificados están adecuadamente protegidas según lo descrito en el punto 2.6 de esta Declaración de Prácticas de Certificación (CPS).

- Las operaciones de alta, modificación o baja de registros por parte de los operadores remotos de las Autoridades de Registro están protegidas mediante el acceso con certificado digital gestionado por una tarjeta de operador.
- Las operaciones de envío de peticiones de certificación por parte de los solicitantes están protegidas mediante una contraseña de acceso previa al envío.
- El proceso se describe en el capítulo 4 de este documento.

MEDIDAS PARA GARANTIZAR EL NIVEL DE SEGURIDAD

Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad y que se encuentran descritas en los documentos que conforman la política de protección de datos y seguridad de la información del Consejo General de la Abogacía