Autoridad de Certificación de la Abogacía

Referencia: **CPS_ACA_001.1**
Fecha: 0**2/03/2004**
Estado del documento: **Publicado**

Consejo General de la Abogacía Española

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN (CPS) DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

CERTIFICADOS CORPORATIVOS

Esta versión está basada en las
Políticas y Prácticas de Certificación de la
Jerarquía de Certificación de
Firmaprofesional, S.A.
(versión 2.0)

firmaprofesional
http://www.firmaprofesional.com

DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN DEL LA ABOGACÍA (AC ABOGACÍA)

Control del Cambios

Fecha	Versión	Cambios
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.

Resumen de los derechos y obligaciones fundamentales contenidos en esta CPS

ESTE TEXTO ES UNA MERA SÍNTESIS DEL CONTENIDO COMPLETO DE LA 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 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 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/index.htm 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 CPS y en las correspondientes Prácticas 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 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 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 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 certificados de la cadena de confianza son válidos y no han caducado o han sido suspendidos o revocados.

- En la 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.

Para más información, consulte nuestra página web en la dirección http://www.acabogacia.org o póngase en contacto con nosotros a través de la siguiente dirección de e-mail info@acabogacia.org

Índice de Contenido

1. Introducción

1.1. Presentación

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 Certificación mediante la contratación de los servicios de la sociedad Firmaprofesional, S.A., para dotarse de la infraestructura necesaria para la consecución del proyecto, estableciendo una CA específica de la Abogacía dentro de la jerarquía de certificación de Firmaprofesional.

Firmaprofesional S.A. nació como un proyecto de diversos colegios profesionales y se constituyó en el año 2001, como Sociedad Anónima con el fin de actuar con total independencia como Autoridad de Certificación Digital de los Colegios Profesionales. Firmaprofesional eligió como socio tecnológico a AC Camerfirma, S.A., entidad de certificación de las Cámaras de Comercio, con quien firmo un contrato de outsourcing tecnológico.

El CGAE ha desarrollado una Entidad de Certificación propia de la Abogacía utilizando toda la experiencia previa de Firmaprofesional, y en especial, la experiencia adquirida por este organismo en su colaboración con otras corporaciones profesionales. Esta elección ahonda más en una de las claves del Proyecto de Firma Electrónica de la Abogacía: la homogeneidad frente a la diversidad y el carácter “colegial” y adaptado a las necesidades del profesional.

1.1.1 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 personales, y está basada en la especificación del estándar RCF 2527 – *Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*, de IETF y en las propias políticas de certificación del CGAE (*vea "Política General de Certificación del Consejo General de la Abogacía Española", en http://www.acabogacia.org/doc/index.htm"*), siguiendo su misma estructura.

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 Prestadores de Certificación Acreditados.

Esta 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 CPS y que a su vez ha sido aprobadas en virtud de las políticas de la jerarquía de Firmaprofesional (*vea "Política de Certificación - Root CA de Firmaprofesional", en http://www.firmaprofesional.com/doc/index.htm"*). 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 CPS y por las políticas citadas, establece la emisión de dos clases principales de certificados:

1. CERTIFICADO DE COLEGIADO. Son certificados de tipo Corporativo expedidos a entidades finales, personas físicas pertenecientes a un Colegio de Abogados, es decir, emitidos con la intervención de su Colegio de Abogados, en calidad de Registrador con la capacidad exclusiva de certificar la cualidad de "colegiado" de una persona identificada en el certificado.

2. CERTIFICADO DE PERSONAL ADMINISTRATIVO. Son certificados de tipo Corporativo expedidos a entidades finales, personal vinculado funcionalmente a los Colegios de Abogados, Consejos Autonómicos de Colegios de Abogados y el Consejo General de la Abogacía Española, que actúan como Registradores, o a instituciones vinculadas con estos.

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 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.

La actividad de la AC podrá ser sometida a la inspección de la Autoridad de Políticas (PA) de la jerarquía de certificación de Firmaprofesional o por personal delegado por la misma.

En lo que se refiere al contenido de esta 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

Nombre:	CPS_ACA_001
Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Versión:	001.1
Fecha de Emisión:	27/03/2003
Fecha Revisión:	02/03/04
Localización:	www.acabogacia.org/doc/index.htm

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, en la jerarquía de certificación de Firmaprofesional.

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

1.3.2 Prestador de servicios de certificación (PSC).

Entendemos bajo la presente CPS a un PSC como aquella entidad que presta servicios concretos relativos al ciclo de vida de los certificados.

Las funciones de PSC pueden ser desempeñadas directamente por la AC o por una entidad delegada.

A los efectos de la presente CPS, el CGAE es el PSC en el ámbito de la emisión, publicación de certificados y listas de certificados revocados, siendo Firmaprofesional la Autoridad de Certificado Raíz dentro la jerarquía de certificación. Es decir, AC Abogacía es la entidad emisora de los certificados y responsable de las operaciones del ciclo de vida

de los certificados, excepto las citadas previamente, y Firmaprofesional el fabricante de dichos certificados y el proveedor de los sistemas de gestión de los certificados.

1.3.3 Autoridad de Registro (AR)

A los efectos de la presente CPS podrán actuar como AR's 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)

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.

1.3.4 Suscriptor

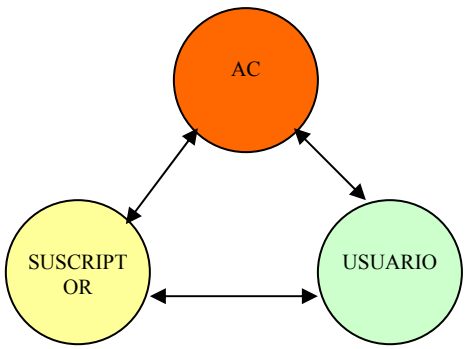
De acuerdo a la presente CPS podrán emitirse certificados digitales de la AC Abogacía a las siguientes personas físicas:

- Para los certificados de Colegiado: personas pertenecientes a un Colegio Profesional en calidad de colegiado.

- Para los certificados de Personal Administrativo: personas pertenecientes a un Colegio o Consejo de Colegios de Abogados en calidad de empleados o vinculados a los mismos o a una empresa vinculada al mismo.

1.3.5 Usuario

En esta CPS se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el Certificado de AC Abogacía, en virtud de la confianza depositada en la AC. Se establece por tanto un círculo de confianza a tres partes.



1.3.6 Solicitante

El solicitante es el sujeto que se encuentra en un estado previo a la obtención del certificado y posterior a su solicitud.

1.3.7 Ámbito de Aplicación y Usos

La presente CPS da respuesta a las siguientes políticas de certificación, que se pueden encontrar en www.acabogacia.org/doc/index.htm:

Política de Certificado de Colegiado (OID 1.3.6.1.4.1.16533.1.1. 1)
Política de Certificado de Personal Administrativo (OID 1.3.6.1.4.1.16533.1.1.2)

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

1.3.7.1 Usos Prohibidos y no Autorizados

Se prohíbe el uso de los certificados según lo dispuesto en las políticas de certificación correspondientes

1.4. Datos de contacto

Organización responsable:
Autoridad de certificación de la Abogacía.
Consejo General de la Abogacía Española

Persona de contacto:
Administrador AC Abogacía
Departamento de Operaciones

E-mail:	info@acabogacia.org
Teléfono:	Tel. 91 523 25 93
Dirección:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

2. Cláusulas Generales

2.1. Obligaciones

2.1.1 AC

La AC se obliga según lo dispuesto en las Políticas de Certificación y en esta CPS, principalmente:

1. Respetar lo dispuesto en las Políticas de Certificación.
2. Proteger sus claves privadas de forma segura.
3. Emitir certificados conforme a esta Política y a los estándares de aplicación.
4. Emitir certificados según la información que obra en su poder y libres de errores de entrada de datos.
5. Emitir certificados cuyo contenido mínimo sea el definido por la normativa vigente.
6. Publicar los certificados emitidos en un Registro de Certificados, respetando en todo caso lo dispuesto en materia de protección de datos por la normativa vigente.
7. Suspender y revocar los certificados según lo dispuesto en la CPS y publicar las mencionadas revocaciones en la CRL (Lista de Certificados Revocados).
8. Informar a los Suscriptores de la revocación o suspensión de sus certificados, en tiempo y forma de acuerdo con la legislación Española vigente.
9. Publicar esta CPS en su página web.
10. 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.
11. No almacenar ni copiar los datos de creación de firma del Suscriptor.
12. Proteger, con el debido cuidado, los datos de creación de firma mientras estén bajo su custodia si así se contemplase.
13. Establecer los mecanismos de generación y custodia de la información relevante en las actividades descritas, protegiéndolas ante pérdida, destrucción o falsificación.
14. Disponer de un seguro de responsabilidad civil que debe cubrir un valor mínimo en la medida en que sea exigible por la normativa vigente.
15. Conservar la información sobre el certificado emitido por el período mínimo exigido por la normativa vigente.

2.1.2 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:

1. Respetar lo dispuesto en esta CPS.
2. Comprobar la identidad de los solicitantes de certificados.
3. Verificar la exactitud y autenticidad de la información suministrada por el Suscriptor solicitante.
4. Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el suscriptor.
5. Respetar lo dispuesto en los contratos firmados con la AC.
6. Respetar lo dispuesto en los contratos firmados con el Suscriptor.
7. Informar a la AC las causas de revocación, siempre y cuando tomen conocimiento.

2.1.3 Solicitante

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

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

2.1.4 Suscriptor

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

1. Custodiar su clave privada de manera diligente.
2. Usar el certificado según lo establecido en la presente CPS y las Políticas de Certificación aplicables.
3. Respetar lo dispuesto en los documentos firmados con la AC y la AR.
4. Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.

5. Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

6. 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.

2.1.5 Usuario

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

1. Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.

2. Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía, y aceptar sujetarse a las mismas.

2.1.6 Registro de Certificados

La información relativa a la emisión y el estado de los certificados se mantendrá accesible al público en los términos establecidos en la normativa vigente.

La AC mantendrá un sistema seguro de almacén y recuperación de certificados y un Registro de Certificados 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).

2.2. Responsabilidad

La AC será responsable del daño causado ante el Suscriptor o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, 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.

2.2.1 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 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. Estado de Guerra, desastres naturales o cualquier otro caso de fuerza mayor.

2. Por el uso de los certificados siempre y cuando exceda de lo dispuesto en la normativa vigente y la presente 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.

3. Por el uso indebido o fraudulento de los certificados o CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.

4. Por el uso indebido de la información contenida en el Certificado o en la CRL.

5. Por el incumplimiento de las obligaciones establecidas para el Suscriptor o Usuarios en la normativa vigente, la presente CPS o en la Política de Certificación correspondiente.

6. Por el perjuicio causado en el periodo de verificación de las causas de revocación /suspensión.

7. Por el contenido de los mensajes o documentos firmados o encriptados digitalmente.

8. Por la no recuperación de documentos cifrados con la clave pública del Suscriptor.

9. Fraude en la documentación presentada por el solicitante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

La AC limita su responsabilidad mediante la inclusión de los límites de uso del certificado, y límites del valor de las transacciones para las cuales pueden emplearse los mismos, expresadas en los propios certificados y en las Políticas y Prácticas de Certificación.

El límite monetario del valor de las transacciones se expresa en el propio certificado mediante la inclusión de una extensión "qcStatements", (OID 1.3.6.1.5.5.7.1.3), tal como se define en la RFC 3039. La expresión del valor monetario se ajustará a lo dispuesto en la sección 4.2.2 de la norma TS 101 862 de la ETSI (European Telecommunications Standards Institute, *www.etsi.org).*

2.3. Responsabilidad financiera

Firmaprofesional, en su actividad como prestador de servicio a la AC Abogacía dispone de 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 PSC tal como se define en la legislación española vigente.

2.4. Interpretación y ejecución

2.4.1 Legislación

La ejecución, interpretación, modificación o validez de la presente CPS se regirá por lo dispuesto en la legislación española vigente.

2.4.2 Independencia

La invalidez de una de las cláusulas contenidas en esta CPS no afectará al resto del documento. En tal caso se tendrá la mencionada cláusula por no puesta.

2.4.3 Notificación

Cualquier notificación referente a la presente CPS se realizará por correo electrónico o mediante correo certificado dirigido a cualquiera de las direcciones referidas en el apartado datos de contacto.

2.4.4 Procedimiento de resolución de disputas

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el 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.

2.5. Tarifas

2.5.1 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.

2.5.2 Tarifas de acceso a los certificados

El acceso a los certificados emitidos es gratuito, no obstante, la AC se reserva el derecho de 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.

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

La AC provee un acceso a la información relativa al estado de los certificados o de los certificados revocados gratuito, por medio de la publicación de la CRL. No obstante, la AC se reserva el derecho de imponer alguna tarifa para otros medios de comprobación del estado de los 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.
.

2.5.4 Tarifas por otros servicios

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

2.5.5 Política de reintegros

Sin estipulación.

2.6. Publicación y Registro de Certificadoss

2.6.1 Publicación de información de la AC

2.6.1.1 Políticas y Prácticas de Certificación

La presente CPS actual y sus distintas versiones están disponibles públicamente en el sitio de Internet http://www.acabogacia.org/doc/index.htm.

2.6.1.2 Términos y condiciones

AC Abogacía pone a disposición de los Suscriptores y Usuarios los términos y condiciones del servicio en el sitio de Internet http://www.acabogacia.org/doc/index.htm.

2.6.1.3 Difusión de los 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.

2.6.2 Frecuencia de publicación

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

AC Abogacía publica los certificados en el Registro de Certificados inmediatamente después de haber sido emitidos y siempre tras la aprobación del suscriptor.

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

2.6.3 Controles de acceso

AC Abogacía emplea entre otros sistemas un directorio LDAP para la publicación y distribución de certificados y CRL's. Para salvaguardar la información almacenada, no se permiten búsquedas y accesos masivos a este directorio. Se necesita tener unos datos de acceso para realizar estas operaciones.

En la Web de AC Abogacía existen 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 pueden descargarse de forma anónima mediante protocolo http desde la siguiente dirección:

http://crl.firmaprofesional.com/acabogacia.crl

2.7. Auditorias

2.7.1 Frecuencia de las auditorías

Se realiza una auditoria con carácter anual.

2.7.2 Identificación y calificación del auditor

Las auditorías son realizadas por parte de Ernst&Young, 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).

2.7.3 Relación entre el auditor y la AC

Ernst&Young es 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 o Firmaprofesional.

No obstante, Firmaprofesional realiza auditorias periódicas internas a las AC de la jerarquía para garantizar en todo momento su adecuación a los requerimientos marcados por las políticas de certificación de la jerarquía.

2.7.4 Tópicos cubiertos por la auditoría

La auditoria verifica los siguientes principios:

a) Publicación de la Información: Que la AC hace públicas las Prácticas de Negocio y de Gestión de Certificados, así como la política de privacidad de la información y proporciona sus servicios conforme a dichas afirmaciones.
b) Integridad de Servicio. Que la AC mantiene controles efectivos para asegurar razonablemente que:
    i. La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la AC), y
    ii. La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.
c) Controles generales. Que la AC mantiene controles efectivos para asegurar razonablemente que:
    i. 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.
    ii. Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.
    iii. 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.

2.7.5 Auditoría en las Autoridades de Registro

Todas las Autoridades de Registro son auditadas previamente a su puesta en marcha efectiva. Adicionalmente, se realizan auditorias anualmente 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.

Las auditorias a las Autoridades de Registro las realiza una tercera parte.

2.7.6 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.

2.8. Confidencialidad

2.8.1 Tipo de información a mantener confidencial

AC Abogacía y Firmaprofesional considerarán 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 la haya otorgado el carácter de confidencialidad, a no ser que exista una imposición legal.

AC Abogacía y Firmaprofesional disponen 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.

AC Abogacía y Firmaprofesional cumplen en todo caso con la normativa vigente en materia de protección de datos y concretamente con lo dispuesto por la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal.

2.8.2 Tipo de información considerada no confidencial

AC Abogacía y Firmaprofesional consideran como información no confidencial:

a) La contenida en la presente CPS y en las Políticas de Certificación.
b) La información contenida en los certificados siempre que el Suscriptor haya otorgado su consentimiento.
c) Cualquier información cuya publicidad sea impuesta normativamente.

La siguiente información será considerada no confidencial, y de esta forma será reconocido por los afectados, en el documento jurídico vinculante con la AC:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por el Prestador de Servicios de Certificación.
- El nombre y los apellidos del suscriptor del certificado, en caso de certificados individuales, así como cualesquiera 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.
- Toda otra información que no esté indicada en la sección anterior de esta política.

2.8.3 Divulgación de información de revocación / suspensión de certificados

AC Abogacía difunde la información relativa a la suspensión o revocación de un certificado mediante la publicación periódica de las correspondientes CRLs.

Se dispone de un servicio de consulta de CRL y Certificados en la dirección http://www.acabogacia.org.

2.8.4 Envío a la Autoridad Competente

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

2.9. Derechos de propiedad intelectual

La propiedad intelectual de esta CPS pertenece al CGAE sin perjuicio de los derechos de propiedad intelectual de Firmaprofesional, S.A. sobre la CPS de la jerarquía de certificación de ésta última, en la que está basada, constituyendo una adaptación a las especificidades propias de AC Abogacía.

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.

Las anteriores reglas figurarán en los instrumentos vinculantes entre AC Abogacía y los suscriptores y los terceros que confían en certificados.

3. Identificación y Autenticación

3.1. Registro inicial

3.1.1 Tipos de nombres

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

El DN de los certificados Corporativos contendrá como mínimo los elementos que se citan con el formato siguiente. Todos los valores de los componentes serán autenticados por la Autoridad de Registro:

- Un componente Nombre (Common Name) –CN
- Un componente E-mail –E
- Un componente Organización –O
- Un componente Unidad en la Organización –OU
- Un componente Título-T
- Un componente de ubicación geográfica -ST
- Un componente Estado (Country)-C
- Un componente Número de Serie -serialNumber

Certificados de Colegiado

- El valor autenticado del componente Nombre (Common Name) –CN contendrá el nombre (Nombre y Apellidos) y numero de NIF o NIE del suscriptor
- El valor autenticado del componente E-mail –E contendrá la dirección de correo electrónico del suscriptor
- El valor autenticado del componente Organización –O contendrá el nombre del Registrador, es decir el Colegio de Abogados al que pertenezca el suscriptor, y una referencia al código identificativo de la AR
- El valor autenticado del componente Unidad en la Organización –OU contendrá el Código postal de la sede principal del registrador y el numero de colegiado del suscriptor

- El valor autenticado del componente Título-T contendrá el titulo, especialidad, rol o membresía profesional del suscriptor

- El valor autenticado del componente de ubicación geográfica -ST contendrá una referencia al ámbito geográfico de colegiación del suscriptor

- El valor autenticado del componente Estado (Country)-C contendrá "ES"

- El valor autenticado del componente Número de Serie –serialNumber contendrá el NIF o NIE del suscriptor.

Certificados de Personal Administrativo

- El valor autenticado del componente Nombre (Common Name) –CN contendrá el nombre (Nombre y Apellidos) y numero de NIF o NIE del suscriptor.

- El valor autenticado del componente E-mail –E contendrá la dirección de correo electrónico del suscriptor

- El valor autenticado del componente Organización –O contendrá el nombre de la institución con la cual el suscriptor mantiene la vinculación, es decir el Colegio o Consejo de Abogados o empresa vinculada a estos al que pertenezca el suscriptor, y una referencia al código identificativo de la AR

- El valor autenticado del componente Unidad en la Organización –OU contendrá el Departamento o Unidad al que pertenezca el suscriptor

- El valor autenticado del componente Título-T contendrá el cargo, titulo o rol del suscriptor en la organización

- El valor autenticado del componente de ubicación geográfica -ST contendrá una referencia al ámbito geográfico de vinculación del suscriptor

- El valor autenticado del componente Estado (Country)-C contendrá "ES"

- El valor autenticado del componente Número de Serie –serialNumber contendrá el NIF o NIE del suscriptor.Adicionalmente, se incluirá un componente CIF de la Organización, representado por el siguiente OID (1.3.6.1.4.1.4710.1.3.2), que contendrá el CIF correspondiente a la institución vinculada al suscriptor.

3.1.2 Pseudónimos

En ningún caso se pueden emplear anónimos. Tampoco se pueden emplear seudónimos para identificar a una organización. Los certificados corporativos de colegiado no admiten seudónimos. Los certificados corporativos de personal administrativo sólo admiten el empleo de roles en lugar del nombre real.

3.1.3 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.

3.1.4 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.

3.1.5 Procedimiento de resolución de disputas 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. El Prestador de Servicios de Certificación 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.

El Prestador de Servicios de Certificación 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 2.4.4 de esta 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.

3.1.7 Métodos de prueba de la posesión de la clave privada

La clave privada es generada por el suscriptor y permanece en todo momento en posesión exclusiva del mismo. El suscriptor crea la pareja de claves privada y pública, y posteriormente envía una petición de emisión de certificado válida a AC Abogacía, que emite el certificado con la clave pública del suscriptor que esta asociada matemáticamente a la clave privada que el suscriptor mantiene bajo su custodia.

El método de prueba de la posesión de la clave privada por el suscriptor es PKCS#10 o una prueba criptográfica equivalente u otro método aprobado por AC Abogacía y Firmaprofesional

3.1.8 Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del suscriptor de certificados personales, se exigirá la personación física del suscriptor ante la AR y la presentación del Documento Nacional de Identidad, tarjeta de residencia, pasaporte u otro medio reconocido en derecho y que identifique a la persona ante un operador o personal debidamente autorizado de la Autoridad de Registro.

La AR verificará con sus propias fuentes de información el resto de datos y atributos a incluir en el certificado (nombre distinguido del certificado), debiendo guardar la documentación acreditativa de la validez de aquellos datos que no puede comprobar por medio de sus propias fuentes de datos.

Lo dispuesto en los párrafos anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la AR en virtud de una relación preexistente, en la que, para la identificación del interesado, se hubieran empleado los medios señalados en el párrafo primero y el período de tiempo transcurrido desde la identificación es menor de cinco años.

b) Cuando para solicitar un certificado se utilice otro para cuya expedición se hubiera identificado al firmante en la forma prescrita en el párrafo primero y le conste a la AR que el período de tiempo transcurrido desde la identificación es menor de cinco años.

3.1.9 Autenticación de la identidad de Operadores de la Autoridad de Registro

Las Autoridades de Registro son los propios Colegios y Consejos de Colegios de Abogados de España, por lo que la identidad de estos no necesita ser comprobada ante el Consejo General de la Abogacía Española.

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, concretando 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.
- 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.

Para realizar una correcta identificación de la identidad del operador, AC Abogacía exigirá la personación física ante un administrador o persona autorizada por la AC y la presentación del Documento Nacional de Identidad, tarjeta de residencia, pasaporte u otro documento que legalmente identifique a la persona. Adicionalmente, será necesario aportar un documento emitido por un representante capacitado de la Autoridad de Registro que acredite la autorización del individuo para actuar como operador de la Autoridad de Registro.

3.2. Renovación de certificados

La renovación de certificados consiste en la emisión de un nuevo certificado al suscriptor a la fecha de caducidad del certificado original. Antes de renovar un certificado, la AR deberá comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor continúan siendo válidos.

Si cualquier información del suscriptor hubiere cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.1.8.

3.3. Reemisión después de una revocación

La emisión de un nuevo certificado a un suscriptor tras la revocación del certificado previo se tratará de acuerdo con lo establecido en la sección 3.1.8. 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. 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 según lo establecido en el apartado 3.1.8.

- 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

4.1. Solicitud de certificados

Las AR's gestionan las solicitudes de Certificados de Colegiado y Certificados de Personal Administrativo.

La AC gestiona las solicitudes de los certificados internos de administración y operación.

El circuito de emisión comienza por la existencia de una solicitud en estado "No Iniciado" disponible en el sistema de gestión de solicitudes de la AC. Esta solicitud puede haberla generado de la AR tras una petición del solicitante.

La AR comunica al solicitante la disponibilidad para realizar el proceso de registro.

El solicitante acude a la AR donde se le informa del proceso de emisión, las responsabilidades y las condiciones de uso del certificado y del dispositivo.

La AR verifica la identidad del solicitante, y los datos a incluir en el certificado.

Si la verificación es correcta se procede a la firma del instrumento jurídico vinculante entre el solicitante y la AC – AR, convirtiéndose el solicitante en suscriptor.

La AR le hace entrega (si no dispone de él) de un kit conteniendo el dispositivo criptográfico (generalmente una tarjeta inteligente) de soporte de la clave privada y los dispositivos de acceso a el, si los hubiera (generalmente un lector de tarjetas inteligentes).

Si el dispositivo no hubiere sido previamente inicializado, el suscriptor inicializa en la propia AR y ante el operador el dispositivo criptográfico con lo que el estado de la solicitud cambia a "En Proceso". Durante el proceso de inicialización se generan los datos de activación del dispositivo y de acceso a la clave privada que contendrá. El suscriptor generará los datos de activación, 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 en su dispositivo criptográfico, y crea una contraseña de revocación del certificado a emitir, enviando por un canal seguro la clave publica 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.

La AC notifica al suscriptor que ha recibido una petición a su nombre.

4.2. Emisión de certificados

El proceso seguido para la emisión de certificados es el siguiente:

- La AR recibe la petición de emisión del certificado, en estado "Petición de certificación sin firmar".
- El operador de la AR verifica nuevamente el contenido del mismo y si la verificación es correcta lo valida y tramita la aprobación de la emisión para la AC, mediante la firma digital de la petición con su certificado de operador. En ese momento la petición pasa a estado "Petición de certificación validada". Si la petición no es correcta y el defecto es subsanable, el operador de la AR modifica los datos, valida nuevamente y tramita la petición. Si el defecto es no subsanable, el operador deniega la petición.
- La AR notificará al suscriptor que la petición ha sido aprobada, modificada o denegada.
- El operador envía por un canal seguro la petición a la AC para la emisión del correspondiente certificado.
- La AC emite el certificado, si la petición recibida no contiene errores técnicos, en el formato o contenido de la misma, vinculando de forma segura el certificado con la información de registro, incluyendo la clave pública certificada, en un sistema que utiliza protección contra falsificación y mantiene la confidencialidad de los datos intercambiados.
- El certificado generado es enviado de forma segura a la AR, que lo pone a disposición del suscriptor.
- La AC notifica al suscriptor la emisión del mismo y el método de descarga.
- El certificado generado es enviado de forma segura al Registro de Certificados, que lo pone a disposición de los usuarios.

4.3. Aceptación de certificados

Un suscriptor acepta su certificado cuando descarga su certificado en el dispositivo criptográfico que custodia la clave privada, mediante el acceso al sistema de descarga de certificados de la AC-AR y efectúa los pasos técnicos que el sistema provee para la descarga.

Sin perjuicio de lo indicado en el párrafo anterior, el suscriptor dispone de un periodo máximo de siete días naturales para notificar a la AR cualquier defecto en los datos del certificado, o en la publicación de los datos del mismo en el Registro de Certificados de certificados.

4.4. 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.
Las revocaciones y suspensiones tienen efecto desde el momento en que aparecen publicadas en la CRL.

4.4.1 Causas de revocación de certificados

La AC podrá revocar un certificado debido a 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.
- Pérdida del suscriptor de condición de colegiado.
- Pérdida o cambio del suscriptor de la vinculación con la institución, en el caso de Certificados de Personal Administrativo

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

- Compromiso de la clave privada o de la infraestructura o sistemas del 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 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 CPS o en el instrumento jurídico vinculante entre la AC, la AR y el suscriptor.

3. Circunstancias que afectan a la seguridad del dispositivo criptográfico

- Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.
- Pérdida o inutilización por daños del dispositivo criptográfico.
- Acceso no autorizado, por un tercero, a los datos de activación del suscriptor.
- El incumplimiento por parte del suscriptor de las normas de uso del dispositivo criptográfico expuestas en las políticas, en la CPS o en el instrumento jurídico vinculante entre la AC, la AR y el suscriptor.

4. Circunstancias que afectan al suscriptor

- 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 CPS de la AC.
- La incapacidad sobrevenida, total o parcial.
- Por el fallecimiento del suscriptor.

5. Otras circunstancias

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

Si la AR ó 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. En este caso se considerará que el uso del certificado realizado durante el período de suspensión no es válido, siempre y cuando el certificado finalmente sea revocado. Será válido si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido.

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.

4.4.2 Quién puede solicitar la 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 según lo establecido en el apartado 3.1.8.
- Los operadores autorizados de la AR del suscriptor
- Los operadores autorizados de la AC o de la jerarquía de certificación.

- Los Administradores autorizados de la AC o de la jerarquía de certificación.

4.4.3 Procedimiento de solicitud de revocación o suspensión

El procedimiento de solicitud de revocaciones o suspensiones presenta puede iniciarse por víapresencial, telefónica u online, 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, mediante formato preparado al efecto, 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.

- Revocación 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, o la revocación del certificado. Asimismo, enviará un mensaje al suscriptor comunicándole la circunstancia.

Procedimiento telefónico (Call Center de Revocación de Firmaprofesional):

El procedimiento de revocación se iniciará a partir de una llamada telefónica. El teléfono de atención telefónica de la AC Abogacía eso **902.41.11.41**, adicionalmente existe un servicio habilitado de forma específica para el caso **902.361.639**.

En función de la persona que solicita la revocación, se desarrollaran dos procedimientos diferentes:

- *Revocación por parte del suscriptor*: el operador que atienda la llamada se conectará al sistema de suspensión y le pedirá al suscriptor el código de revocación. Si este código es correcto, el operador del call centre suspenderá el certificado y enviará un mensaje de comunicación a la AR, con los datos de suspensión y el motivo.

  En el caso de que, el suscriptor no conozca la clave de revocación o no quiera decirla, el call centre tramitará el proceso como si actuara un tercero.

- *Revocación por parte de un tercero*: En el caso de ser un tercero o un suscriptor que no conoce la clave de revocación de su certificado, el operador le realizará una serie de preguntas para eliminar la posibilidad de intento de revocaciones masivas, en el caso de que el call centre tenga certeza razonable de que el tercero conoce al suscriptor o tiene en su poder el dispositivo criptográfico, el call centre suspenderá preventivamente el certificado y le comunicará al tercero que puede acudir a la AR para formalizar la revocación del certificado. Asimismo, enviará un mensaje de comunicación, a la AR, con los datos de suspensión y el motivo.

Al tiempo de suspenderse el certificado, se enviará un comunicado al suscriptor, comunicando la hora de suspensión y la causa de la misma.

La AR recibirá un correo del sistema informándole que se ha producido una suspensión del certificado, y en función de la información contenida en el correo el Operador actuará de dos maneras:

a) Si ha solicitado la revocación el propio suscriptor: no entrará a conocer más datos y procederá dar la orden de revocación a la AC.

b) Si ha solicitado la revocación un tercero: la AR realizará las averiguaciones pertinentes, solicitando al suscriptor o a terceros la documentación acreditativa de la circunstancia que motivó la solicitud, y finalmente decidirá y procederá la revocación definitiva o el levantamiento de la suspensión.

Al tiempo de revocarse el certificado, se enviará un aviso al suscriptor comunicando la hora de revocación y la causa de la misma.

Procedimiento online (http://www.acabogacia.org/suscriptores/revocacion.asp):

El suscriptor dispondrá de una página web en www.acabogacia.org desde la que podrá solicitar la revocación de su certificado.
Para ello, deberá:

- Acceder a https://www.acabogacia.org/suscriptores/revocacion.asp .
- En el formulario dispuesto escribir correctamente sus datos identificativos.
- Introducir el Código de Revocación proporcionado durante el proceso de generación del certificado.
- Introducir la causa de solicitud de revocación.
- Aceptar explícitamente la tramitación de la solicitud y las consecuencias de ésta.

El sistema suspenderá el certificado. Al tiempo de suspenderse el certificado, se notificará al suscriptor, comunicando la hora de suspensión y la causa de la misma.

La AR recibirá un correo del sistema informándole que se ha producido una suspensión del certificado, y en función de la información contenida en el correo el Operador no entrará a conocer más datos y procederá dar la orden de revocación a la AC.

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.

4.4.4 Periodo de revocación

La decisión de revocar o no un certificado 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.

4.4.5 Suspensión

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

Si la AR ó 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 ó 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 3280). En algunas aplicaciones del sistema operativo Microsoft Windows, al consultar una lista de certificados revocados, dicha causa aparece traducida como “Posesión de certificado (6)”, lo cual puede inducir a error en el usuario.

4.4.6 Quién puede solicitar la suspensión

Ver 4.4.2.

4.4.7 Procedimiento para la solicitud de suspensión

Ver 4.4.3

4.4.8 Límites del periodo de suspensión

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

4.4.9 Frecuencia de emisión de CRL's

La AC raíz de la jerarquía de certificación de Firmaprofesional emitirá una CRL cada vez que se revoca el certificado de una AC en la jerarquía. En todo caso emitirá una CRL con una frecuencia al menos mensual.

La AC Abogacía emitirá una nueva CRL con una periodicidad de 24 horas. La CRL indicará el momento programado de emisión de una nueva CRL, si bien se podrá emitir una CRL antes del plazo indicado en la CRL anterior.

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

Los certificados revocados que expiren podrán ser retirados de la CRL transcurridos un mínimo de sesenta días naturales desde la expiración.

.

4.4.10 Obligación de comprobación de CRL's

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 la siguiente dirección http://crl.firmaprofesional.com/acabogacia.crl.

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 esta firmada por la autoridad que ha emitido el certificado que quiere validar.

4.4.11 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.

4.4.12 Requisitos de la comprobación del estado de los certificados

Para realizar la comprobación del estado de un certificado el usuario deberá conocer el e-mail del suscriptor o el número de serie asociado al certificado que desea verificar.

4.4.13 Obligación de consulta del servicio de comprobación del estado de los certificados

El usuario que no utilice la CRL para comprobar la validez de un certificado deberá consultar el Registro de Certificados para confiar en él.

4.4.14 Otras formas de divulgación de información de revocación disponibles

No estipulado.

4.4.15 Requisitos de comprobación para otras formas de divulgación de información de revocación

No estipulado.

4.4.16 Requisitos especiales de revocación por compromiso de las claves

En el caso de compromiso de las claves de la AC, este hecho será notificado en la medida de lo posible a todos los participantes en la jerarquía de certificación.

4.5. Procedimientos de Control de Seguridad

4.5.1 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:

- ✓ Encendido y apagado del sistema.
- ✓ Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- ✓ Intentos de inicio y fin de sesión.
- ✓ Intentos de accesos no autorizados al sistema de la AC a través de la red.
- ✓ Intentos de accesos no autorizados a la red interna de la AC.
- ✓ Intentos de accesos no autorizados al sistema de archivos.
- ✓ Acceso físico a los logs.
- ✓ Cambios en la configuración y mantenimiento del sistema.
- ✓ Registros de las aplicaciones de la Autoridad de Certificación.
- ✓ Encendido y apagado de la aplicación de la AC.
- ✓ Cambios en los detalles de la AC y/o sus claves.
- ✓ Cambios en la creación de perfiles de certificados.
- ✓ Generación de claves propias.
- ✓ Eventos del ciclo de vida del certificado.
- ✓ Eventos asociados al uso del módulo criptográfico de la CA.
- ✓ Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente la AC y Firmaprofesional conservan, ya sea manual o electrónicamente, la siguiente información:

- Las ceremonias de creación de claves de la AC y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimiento y cambios de configuración del sistema.
- Cambios en el personal.

- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal de suscriptor, si se gestiona esa información.
- Posesión de datos de activación, para operaciones con la clave privada de la AC.

4.5.2 Frecuencia de procesado de Logs de auditoría

Se revisarán los logs de auditoría cada semana 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.

4.5.3 Periodos de retención para los Logs de auditoría

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

4.5.4 Protección de los Logs de auditoría

Los logs de los sistemas son protegidos de su manipulación mediante la firma de los ficheros que los contienen.

Son almacenados en dispositivos ignífugos.

Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la Autoridad de Certificación.

Los dispositivos son manejados en todo momento por personal autorizado.

4.5.5 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 semanalmente una copia de todos los logs en un medio externo. El medio externo se almacena en armario ignífugo bajo medidas de seguridad que garantizan que su acceso solo está permitido a personal autorizado. Se realizan copias diarias incrementales y completas semanales.

Adicionalmente se mantiene copia de los logs de auditoría en centro de custodia externo.

4.5.6 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.

4.5.7 Notificación al sujeto causa del evento

No estipulado.

4.5.8 Análisis de vulnerabilidades

La AC realiza periódicamente una revisión de discrepancias en la información de los logs y actividades sospechosas, de acuerdo al procedimiento interno establecido al efecto en las políticas de seguridad.

4.6. Archivo de registros

4.6.1 Tipo de eventos registrados

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

- 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 o registros del estado de los certificados generados
- la documentación requerida por los auditores
- las comunicaciones entre los elementos de la PKI

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

4.6.2 Periodo de retención para el archivo

Los certificados se conservarán 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.

4.6.3 Protección del archivo

La AC asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas en los casos en que así se requiera.

La AC dispone de un documento de seguridad donde se detallan todas las acciones tomadas para garantizar la protección de los archivos.

4.6.4 Procedimientos de backup del archivo

La AC dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

4.6.5 Requerimientos para el sellado de tiempo de los registros

Los registros están fechados con una fuente fiable.

Existe dentro del documento de seguridad de la AC un apartado sobre la configuración de tiempos de los equipos utilizados en la emisión de certificados.

4.6.6 Sistema de recogida de información de auditoria

No estipulado.

4.6.7 Procedimientos para obtener y verificar información archivada

Durante la auditoria requerida por esta 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.

4.7. Cambio de clave

Antes de que el certificado de la CA expire se realizará un cambio de claves. La CA antigua y su clave privada solo se usarán para la firma de CRL's mientras existan certificados activos emitidos por la CA antigua. Se generará una nueva CA con una clave privada nueva y un nuevo DN.

Los siguientes certificados se pondrán a disposición pública en el Registro de Certificados:

- Clave publica de la nueva CA firmada por la clave privada de la CA antigua.
- Clave publica de la CA antigua firmada con la clave privada de la nueva CA.

El documento de seguridad de de la AC detalla el proceso de cambio de claves de la AC.

El cambio de claves de usuario es realizado mediante la realización de un nuevo proceso de emisión.

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

La AC ha desarrollado un plan de contingencias para recuperar todos los sistemas en menos de 48 horas, 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.

4.8.1 La clave de una entidad se compromete

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

En caso de compromiso de la CA, la AC:

- Informará a todos los suscriptores, usuarios y otras AC'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.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

4.8.2 Instalación de seguridad después de un desastre natural u otro tipo de desastre

La AC reestablecerá los servicios críticos (Revocación y publicación de revocados) de acuerdo con esta 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.

La AC dispone de un centro alternativo en caso de ser necesario para la puesta en funcionamiento de los sistemas de certificación.

4.9. Cese de la actividad de la AC

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

Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil) para continuar la finalización de las actividades de revocación.

Informará a todos los suscriptores, usuarios y otras AC's con los cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.

Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.

Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a los suscriptores y usuarios.

La AC mantendrá los certificados activos ya emitidos hasta ese momento y se mantendrá operativo el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos y seis meses más.

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.)
- ✓ Derrumbamiento de la estructura
- ✓ 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 cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso. La localización de las instalaciones garantiza la presencia de fuerzas de seguridad en un plazo no superior a 15 minutos, al encontrarse en el centro urbano de una capital de provincia.

5.1.1 Ubicación y construcción

Las instalaciones de la AC están construidas con materiales que garantizan la protección frente a ataques por fuerza bruta y ubicadas en una zona de bajo riesgo de desastres y permite un rápido acceso.

En concreto, la sala donde se realizan las operaciones criptográficas es una caja de Faraday con protección a radiaciones externas, doble suelo, detección y extinción de incendios, sistemas anti-humedad, doble sistema de refrigeración y sistema doble de suministro eléctrico.

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 del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con detectores de presencia en todos los puntos vulnerables así como Sistemas de alarma para detección de intrusismo con aviso por canales alternativos.

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 automático.

5.1.3 Alimentación eléctrica y aire acondicionado

Las instalaciones de la AC disponen de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado duplicado.

5.1.4 Exposición al agua

Las instalaciones de AC están ubicadas en una zona de bajo riesgo de inundación y en una primera planta. Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Protección y prevención de incendios

Las salas donde se albergan equipos informáticos disponen de sistemas de detección y extinción de incendios automáticos.

5.1.6 Sistema de almacenamiento.

Cada medio de almacenamiento desmontable (cintas, cartuchos, disquetes, etc.), que contenga información clasificada, está etiquetado con el nivel más alto de clasificación de la información que contenga y permanece solamente al alcance de personal autorizado.

La información con clasificación Confidencial, independientemente del dispositivo de almacenamiento se guarda en armarios ignífugos o bajo llave permanentemente en requiriéndose autorización expresa para su retirada.

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 mantiene un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que es independiente del centro operacional.

Se requiere al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2. Controles procedimentales

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. Concretamente:

- Las tareas de Auditor son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.

- Las tareas de Certificación podrán ser realizadas por cuatro personas necesitándose al menos de tres para acceder y activar la clave privada de las CA (una para acceder y dos diferentes para activar). Estas personas no deben formar parte de las tareas de Sistemas.

Las personas implicadas en Administración de Sistemas no podrán ejercer ninguna actividad en las tareas de Auditoría o Certificación.

5.2.2 Numero de personas requeridas por tarea

La AC garantiza al menos dos personas para realizar las tareas que requieren control multipersona y que se detallan a continuación:

Las siguientes tareas requerirán al menos un control dual de personas confiables:

- La generación de la clave de las CA’s.

- La recuperación y back-up de la clave privada de las CA's.
- La emisión de certificados de las CA's.
- Activación de la clave privada de las CA's.
- Cualquier actividad realizada sobre los recursos hardware y software que dan soporte a la root CA.

5.2.3 Identificación y autentificación para cada rol

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que esta asignado.

Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.

El acceso a recursos se realiza dependiendo del activo mediante login/password, certificados digitales, tarjetas de acceso físico y llaves.

5.3. Controles de seguridad de personal

5.3.1 Requerimientos de antecedentes, calificación, experiencia, y acreditación

Todo el personal que realiza tareas calificadas como confiables, lleva al menos dos años trabajando en el centro de producción y tiene contratos laborales fijos.

Todo el personal esta cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas

La AC se asegurará que el personal de registro es personal confiable de un Colegio o del organismo delegado para realizar las tareas de registro.

El empleado del registro habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.

En general la AC retirara de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de estas funciones

5.3.2 Procedimientos de comprobación de antecedentes

Firmaprofesional realiza las investigaciones pertinentes antes de la contratación de cualquier persona. Firmaprofesional nunca asigna tareas confiables a personal con una antigüedad inferior a 6 meses.

5.3.3 Requerimientos de formación

El personal encargado de tareas de confianza ha sido formado en los términos que fija la política de Certificación de la jerarquía.

5.3.4 Requerimientos y frecuencia de la actualización de la formación

La AC y los PSC 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 pudiéndose llegar al cese del trabajador.

5.3.7 Requerimientos de contratación de personal

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

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 practicas 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.

6. Controles de Seguridad Técnica

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 CA y del auditor externo.

La generación de la clave de las CA's delegadas se realiza en un dispositivo que cumple los requerimientos que se detallan en el FIPS 140-1, en su nivel 3.

Las claves son generadas usando el algoritmo de clave pública RSA.

Las claves de las CA's tienen una longitud mínima de 2048 bits.

6.1.1.1 Generación del par de claves del suscriptor

Las claves de los suscriptores y operadores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico FIPS 140-1, nivel 3, un dispositivo ITSEC High4 u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor u operador aportan un nivel de seguridad igual o superior al establecido por la legislación vigente para dispositivos de creación de los datos de firma. La norma europea de referencia para los dispositivos de suscriptor utilizados es CEN CWA 14169.

El dispositivo criptográfico utiliza una clave de activación para el acceso a las claves privadas. En caso de que la entrega del dispositivo no se realice de manera presencial en la AR, los datos de activación se enviarán al lugar de entrega por separado de los dispositivos.

Las claves son generadas usando el algoritmo de clave pública RSA.

Las claves tienen una longitud mínima de 1024 bits.

6.1.2 Entrega de la clave publica 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.

6.1.3 Entrega de la clave pública de la CA a los Usuarios

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

El Fingerprint del certificado digital de la CA de la Autoridad de Certificación de la Abogacía, a las que da cobertura esta CPS es:

Para certificados emitidos antes del 02/03/2004:

SHA -1: 8AA7 EB2C B5DD 1FB5 74BE 59B6 E66C 044B 6F5C AB72

MD-5: 47:24:B3:70:32:0C:22:8C:74:D5:E6:7A:41:79:FA:94

Para certificados emitidos a partir del 02/03/2004:

SHA -1: E529 15B5 B211 2B5E 2092 1051 CFE5 93AA 9422 1031

MD-5: 9C:FB:40:3F:25:D0:7C:29:4F:F0:20:37:4C:9B:74:C5

El Fingerprint de las claves públicas de la CA Raíz de Firmaprofesional a la que se refiere esta CPS es:

SHA -1: A962 8F4B 98A9 1B48 35BA D2C1 4632 86BB 6664 6A8C

MD-5: 11:92:79:40:3C:B1:83:40:E5:AB:66:4A:67:92:80:DF

Los usuarios pueden solicitar la reemisión de una copia autenticada en papel de los datos anteriores en la direcciones de contacto definidas en esta CPS.

6.1.4 Tamaño y periodo de validez de las claves

6.1.4.1 Tamaño y periodo de validez de las claves del emisor

Firmaprofesional emplea claves basadas en el algoritmo RSA con una longitud de 2048 bits en los certificados de CA.

Las claves de CA de la AC abogacía tienen una longitud de 2048 bits.

El periodo de uso de la clave privada de la CA Raíz es de 13 años. El periodo de uso de la clave privada de la CA de AC Abogacía es de 10 años. Las fechas concretas pueden obtenerse de los propios certificados de CA.

6.1.4.2 Tamaño y periodo de validez de las claves del suscriptor

Las claves privadas del suscriptor están basadas en el algoritmo RSA con una longitud de 1024 bits.

El periodo de uso de la clave pública y privada del suscriptor puede ser corresponde con la validez temporal de los certificados, no pudiendo ser en ningún caso superior a 4 años.

6.1.5 Parámetros de generación de la clave pública

No estipulado.

6.1.6 Comprobación de la calidad de los parámetros

No estipulado.

6.1.7 Hardware/software de generación de claves

Las claves de los suscriptores y operadores son generadas por el propio suscriptor de forma segura utilizando un dispositivo criptográfico FIPS 140-1, nivel 3, un dispositivo ITSEC High4 u otro de nivel equivalente.

Los dispositivos criptográficos de custodia de la clave privada del suscriptor u operador aportan un nivel de seguridad igual o superior al establecido por la legislación vigente para dispositivos de creación de los datos de firma. La norma europea de referencia para los dispositivos de suscriptor es CEN CWA 14169.

Las claves de la CA Root son generadas en un en un módulo criptográfico nCipher modelo nFAST validado FIPS 140-1 nivel 2. La CA raíz se encuentra en modo offline y no dispone de tarjeta de conexión a la red.

Las claves de las CA vinculadas son generadas en un módulo criptográfico nCipher modelo nShield validado FIPS 140-1 nivel 3. La CA de la AC Abogacía se encuentra en modo online.

6.1.8 Fines del uso de la clave

Todos los certificados incluyen la extensión Key Usage., indicando los usos habilitados de la claves.

6.2. Protección de la clave privada

Clave privada de la AC

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

La clave privada de firma de la CA raíz es custodiada y utilizada dentro de un almacén seguro PSS encriptado por una clave triple DES, custodiada a su vez por un dispositivo criptográfico hardware que cumple los requerimientos que se detallan en el FIPS 140-1 nivel 2, garantizando que la clave privada nunca está en claro fuera del dispositivo criptográfico. La activación y uso de la clave privada requiere el control multipersona

detallado en el párrafo anterior. Con posterioridad a la operación realizada, la sesión se cierra, quedando desactivada la clave privada.

La clave privada de firma de las CAs Vinculadas es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos que se detallan en el FIPS 140-1 nivel 3.

Cuando la clave privada de la CA está fuera del dispositivo esta se mantiene cifrada y partida en diferentes dispositivos.

Existe un back up de la clave privada de firma de la CA, que es almacenada y recuperada sólo por el personal autorizado según los roles de confianza, usando, al menos un control dual en un medio físico seguro.

Las copias de back up de la clave privada de firma de la CA están almacenadas de forma segura. Este procedimiento se describe en detalle en las políticas de seguridad de Firmaprofesional.

Clave privada del suscriptor

La clave privada del suscriptor se mantiene en un dispositivo criptográfico y es controlada y gestionada por el suscriptor. Tiene un sistema de protección contra intentos de acceso que bloquean el dispositivo cuando se introducen más de tres veces un código de acceso erróneo.

El suscriptor dispone de un código de desbloqueo del dispositivo. Si se introduce tres veces erróneamente, el dispositivo se bloquea definitivamente, quedando inservible.

6.3. Estándares para los módulos criptográficos

Los módulos criptográficos empleados en la CA son homologados FIPS-140-1 nivel 3

6.3.1 Control multipersona (n de entre m) de la clave privada

El acceso a la clave privada de las CA requiere el concurso simultáneo de dos dispositivos criptográficos diferentes de cuatro posibles, protegidos por una clave de acceso. Adicionalmente, el acceso a los dispositivos requiere la presencia de una tercera persona.

6.3.2 Custodia de la clave privada

En ningún caso la AC o Firmaprofesional almacenará la clave privada del suscriptor ni de la CA en el modo llamado de key escrow.

6.3.3 Copia de seguridad de la clave privada

La AC realiza una copia de back up de su propia clave privada de la CA que hace posible su recuperación en caso de desastre o de pérdida o deterioro de la misma.

6.3.4 Archivo de la clave privada

Las claves privadas de las CA's serán archivadas por un periodo no inferior a 10 años después de la emisión del último certificado.

Las claves privadas de los suscriptores pueden ser archivadas por ellos mismos, debido a que pueden ser necesarias para descifrar la información histórica cifrada con la clave publica.

6.3.5 Introducción de la clave privada en el módulo criptográfico

Existe un documento de ceremonia de claves de la CA donde se describen los procesos de generación de la clave privada y el uso del hardware criptográfico.

6.3.6 Método de activación de la clave privada

El acceso a la clave privada del suscriptor se realiza por medio de un PIN (ver apartado 6.2)

Las claves de la CA se activan por un proceso de m de n. Ver apartado 6.3.1

6.3.7 Método de desactivación de la clave privada

La clave privada del suscriptor quedará desactivada una vez se retire el dispositivo criptográfico de creación de firma del dispositivo de lectura.

6.3.8 Método de destrucción de la clave privada

Se destruirán físicamente o reinicializarán a bajo nivel los dispositivos que tengan almacenada cualquier parte de la clave privada de las CAs, o de los datos de activación de las mismas.

6.4. Otros aspectos de la gestión del par de claves

6.4.1 Archivo de la clave pública

La AC conservará todas las claves públicas mientras el servicio de certificación este activo y 6 meses más.

6.4.2 Periodo de uso para las claves públicas y privadas

El periodo de uso de un certificado será determinado por la validez temporal del mismo.
Un certificado no debe ser usado después del periodo de validez del mismo aunque la parte confiante pueda usarlo para verificar datos históricos teniendo en cuenta que no existirá un servicio de verificación válido para ese certificado.

6.5. Ciclo de vida de los dispositivos criptográficos

6.5.1 Ciclo de vida de los dispositivos criptográficos seguro de creación de firma (DSCF)

La AC emplea como DSCF tarjetas con criptoprocesador para que el suscriptor genere y almacene los datos de creación de firma, es decir la clave privada:

a) Las tarjetas son preparadas y estampadas por un proveedor externo de la tarjeta.
b) La gestión de distribución del soporte la realiza el proveedor externo de tarjetas que lo distribuye a las autoridades de registro para su entrega personal al suscriptor. La AR puede realizar una personalización gráfica de la tarjeta.
c) El suscriptor inicializa la tarjeta y la utiliza para generar el par de claves y enviar la clave publica a la CA.
d) La CA envía un certificado de clave pública al suscriptor que es introducido en la tarjeta.
e) La tarjeta es reutilizable y puede mantener de forma segura varios pares de claves.

6.6. Controles de seguridad informática

La AC emplea sistemas fiables y productos comerciales para ofrecer sus servicios de certificación.

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

1. Configuración de seguridad del sistema operativo.
2. Configuración de seguridad de las aplicaciones.
3. Dimensionamiento correcto del sistema.
4. Configuración de Usuarios y permisos.
5. Configuración de eventos de log.
6. Plan de backup y recuperación.
7. Configuración antivirus.
8. Requerimientos de tráfico de red.

El documento de seguridad de Firmaprofesional detalla la arquitectura de los equipos que ofrecen el servicio de certificación tanto en su seguridad física como lógica.

6.6.1 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 auditoria.
- ✓ 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.

6.6.2 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.

La seguridad física esta garantizada por las instalaciones ya definidas anteriormente y la gestión de personal es fácil debido al reducido número de personas que realizan sus trabajos en el centro de datos de Firmaprofesional.

6.7. Controles de seguridad del ciclo de vida

6.7.1 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.

6.7.2 Controles de gestión de la seguridad

6.7.2.1 Gestión de seguridad

La AC desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un foro para la gestión de la seguridad.

La AC exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.7.2.2 Clasificación y gestión de información y bienes

La AC mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la AC detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.

Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL.

6.7.2.3 Operaciones de gestión

La AC dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos. En el documento de seguridad de la AC se desarrolla en detalle el proceso de gestión de incidencias.

La AC dispone de cajas de seguridad ignifugas para el almacenamiento de soportes físicos.

La AC tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad

Todos los soportes serán tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planning del sistema

El departamento técnico de la AC mantiene un registro de las capacidades de los equipos.

Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.

Reportes de incidencias y respuesta

La AC dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades

La AC define actividades asignadas a personas con un rol de confianza distinto a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.7.2.4 Gestión del sistema de acceso

La AC realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas. En particular:

AC General

a) Se dispone de controles basados en firewalls de alta disponibilidad.

b) Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

c) La AC dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

d) La AC dispone de un procedimiento para asegurar que las operaciones se realizan respetando la política de roles.

e) Cada persona tiene asociado su identificador para realizar las operaciones de certificación según su rol.

f) El personal de la AC será responsable de sus actos, por ejemplo, por retener logs de eventos.

Generación del certificado

Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

La autenticación para realizar el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC.

Gestión de la revocación

Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular al sistema de revocaciones.

La revocación se refiere a la perdida de efectividad de un certificado digital de forma permanente. La revocación se realizara mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de log generarán las pruebas que garantizan el no repudio de la acción realizada por el operador de CA.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.7.2.5 Gestión del ciclo de vida del hardware criptográfico

La AC se asegura que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte.

El Hardware criptográfico esta construido sobre soportes preparados para evitar cualquier manipulación.

La AC registra toda la información pertinente del dispositivo para añadir al catalogo de activos del prestador.

El uso del hardware criptográfico de firma de certificados requiere el uso de al menos dos empleados de confianza.

La AC realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.

El dispositivo criptográfico solo es manipulado por personal confiable.

La clave privada de firma de la AC almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.

La configuración del sistema de la AC así como sus modificaciones y actualizaciones son documentadas y controladas.

La AC posee un contrato de mantenimiento del dispositivo para su correcto mantenimiento. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán al menos por dos personas confiables.

6.7.3 Evaluación de la seguridad del ciclo de vida

No estipulado.

6.8. 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.

6.9. Controles de ingeniería de los módulos criptográficos

6.9.1 Módulos criptográficos de la AC

Todas las operaciones criptográficas de la CA son realizadas en un módulo validado por FIPS 140-1 nivel 3.

Almacén del dispositivo criptográfico:

A fin de prevenir la manipulación no autorizada del módulo criptográfico este esta 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 esta 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 de 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 esta 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.

7. Perfiles de Certificado y CRL

7.1. Perfil de Certificado

1.1.1 Preámbulo

Todos los certificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3 , la RFC 3280[1] "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", ETSI TS 101 862[2] conocida como"*European profile for Qualified Certificates"* y la RFC 3039[3] "*Qualified Certificates Profile*". En caso de contradicción prevalecerá lo dispuesto en la norma TS 101 862.

Los certificados corporativos definidos en esta CPS son **certificados reconocidos**, de acuerdo con lo establecido en el art. 2.j) RDL 14/99, con el contenido prescrito por el art. 8 del RDL 14/99, y expedidos siguiendo las prescripciones del art. 12 RDL 14/99. Los certificados corresponden a certificados reconocidos con dispositivo seguro de creación de firma electrónica, de acuerdo con la norma técnica TS 101 456 v1.2.1, del Instituto Europeo de Normas de Telecomunicaciones.

Aclaraciones sobre la extensión "x509v3 KeyUsage" (uso de las claves):
La RFC 3280 que define los perfiles de los certificados X509 sustituye por obsolescencia a la RFC 2459. Un cambio importante es que el uso de la clave "digital signature" como se define en la 3280 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 la nueva RFC 3280.

En estos momentos, existe un borrador de revisión publicado en febrero de 2004 ("*draft5*") de la RFC 3039 con las correcciones adecuadas *(http://www.ietf.org/internet-drafts/draft-ietf-pkix-sonof3039-00.txt)*, en el sentido de que 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.

El resultado de este proceso es probable que afecte a la TS 101 862, puesto que aunque no detalla este aspecto, se refiere al perfil definido en la RFC 3039 objeto de revisión.

El RDL 14/99 y la ley 59/2003 no se manifiesta en absoluto sobre dicha cuestión técnica.

[1] Ver párrafo "Aclaraciones sobre la extensión KeyUsage"
[2] Ídem
[3] Ídem

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 uso "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.

1.1.2 Descripción del perfil

Los certificados tendrán el contenido y campos descritos en esta sección, incluyendo, como mínimo, los siguientes:

CAMPOS	
Versión	V3
(Serial) Nº Serie	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	sha1WithRSAEncryption
(issuer) Emisor	CN = Autoridad de Certificacion de la Abogacia O = Consejo General de la Abogacia NIF Q2863006I OU = Consulte http://www.acabogacia.org L = Paseo de Recoletos 13 Madrid E = ac@acabogacia.org C = ES
(notBefore) Valido desde	(fecha de inicio de validez, tiempo UTC)
(notAfter) Valido hasta	(fecha de fin de validez, tiempo UTC)
(Subject) Asunto	(Según especificaciones de la sección **3.1.1**)

7.1.1 Número de versión

Firmaprofesional emite certificados X.509 Versión 3.

7.1.2 Extensiones del certificado

EXTENSIONES	
X509v3 Subject Alternative Name:	email:<email del suscriptor>
X509v3 Issuer Alternative Name:	URI:http://www.acabogacia.org
X509v3 Basic Constraints: critical	CA:FALSE
X509v3 Key Usage: critical	Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement

X509v3 Extended Key Usage	TLS Web Client Authentication, E-mail Protection
Netscape Cert Type	SSL Client, S/MIME
Netscape CA Policy Url:	http://www. acabogacia.org /doc/index.htm
Netscape Comment	Este es un certificado personal reconocido. Consulte http://www. acabogacia.org/doc/index.htm
X509v3 Subject Key Identifier	(key identifier)
X509v3 Authority Key Identifier	Keyid:(key identifier)
X509v3 CRL Distribution Points	URI:http://crl.firmaprofesional.com/acabogacia.crl
X509v3 Certificate Policies (para Certificado de Colegiado)	Policy: 1.3.6.1.4.1. 16533.1.1.1 URI:http://www.acabogacia.org/doc/1/1.htm User Notice: Explicit Text: Este es un certificado personal reconocido. Consulte http://www.acabogacia.org/doc/index.htm
X509v3 Certificate Policies (para Certificado de personal Administrativo)	Policy: 1.3.6.1.4.1. 16533.1.1.2 URI:http://www.acabogacia.org/doc/1/2.htm User Notice: Explicit Text: Este es un certificado personal reconocido. Consulte http://www.acabogacia.org/doc/index.htm
QcStatements (ver RFC3039)	Límite del valor de las transacciones (ver ETSI TS 101 862)

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. 5 SHA-1 with RSA Encryption

El identificador de objeto del algoritmo de la clave pública es
1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Restricciones de los nombres

No estipulado.

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 3280 "*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.

La CRL se emiten al menos cada 24 horas, o cuando se produzca una revocación, con una validez de 7 días.

7.2.1 Número de versión

Las CRL emitidas por la AC son de la versión 2.

7.2.2 CRL y extensiones

Versión : V2
Emisor : CN = Autoridad de Certificación de la Abogacia; O = Consejo General de la Abogacia NIF Q2863006I; OU = Consulte http://www.acabogacia.org; L = Paseo de Recoletos 13 Madrid; E = ac@acabogacia.org; C = ES
Fecha Efectiva de emisión
Fecha de próxima actualización
Algoritmo de Firma : sha1RSA
Número de CRL
Identificador de la clave de autoridad
Id. de clave= 22 ba 59 71 ac 73 a4 13 6d 3c 18 af f5 d0 82 e3 56 bd 93 b0
Punto de distribución :
URL=http://crl.firmaprofesional.com/acabogacia.crl
Sólo contiene Certificados de usuario=No
Sólo contiene Certificados de la entidad emisora=No
Lista de revocación de certificados (CRL) indirecta=No
Entradas de la CRL
Nº de serie del certificado
Fecha de revocación
Código de razón.

8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1. Autoridad de las políticas

El departamento de operaciones de Firmaprofesional constituye la autoridad de las políticas (PA) de la jerarquía y es responsable de la administración de las CPS. Puede contactar con la PA en:

E-mail:	info@firmaprofesional.com
Teléfono:	Tel. 93.477.42.45
Dirección:	Departamento de Operaciones Firmaprofesional, S.A. Pza. Catalunya s/n "Can Negre" 08970 Sant Joan Despí (Barcelona)

8.2. Procedimientos de especificación de cambios

8.2.1 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.

8.2.2 Cambios con notificación

8.2.2.1 Lista de elementos

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

8.2.2.2 Mecanismo 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.

8.2.2.3 Periodo de comentarios

Los usuarios afectados pueden presentar sus comentarios a la organización de la administración de las políticas dentro de los 45 días siguientes a la recepción de la notificación.

8.2.2.4 Mecanismo de tratamiento de los comentarios

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

8.3. Publicación y copia de la política

Una copia de esta CPS estará disponible en formato electrónico en la dirección de Internet: http://www.acabogacia.org/doc/index.htm. Las versiones anteriores serán retiradas de su consulta on-line, pero pueden ser solicitadas por los interesados en la AC Abogacía.

Los usuarios pueden solicitar una copia de las CPS en formato papel en la dirección de contacto de AC Abogacía.

8.4. Procedimientos de aprobación de la CPS

La publicación de las revisiones de esta CPS deberá ser aprobada por AC Abogacía y la PA, después de comprobar el cumplimiento de los requisitos expresados en las Políticas de Certificación del CGAE y la Política de la Jerarquía de Firmaprofesional.