Autoridad de Certificación de la Abogacía

Referencia: **CPS_ACA_013.0**
Fecha: 11/03/2014
Estado del documento: **Publicado**

Consejo General de la Abogacía Española

CPS_ACA_013.0
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN DE LA AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

(CPS_ACA_013.0)

CPS

CERTIFICADOS CORPORATIVOS

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

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 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

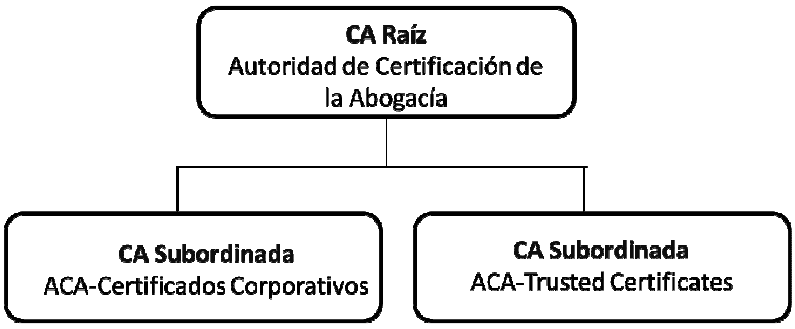
1. Introducción

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 creación de una jerarquía PKI propia.

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



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

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

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.

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. 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 RECONOCIDO DE COLEGIADO. Son certificados, de ámbito nacional y 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 RECONOCIDO DE PERSONAL ADMINISTRATIVO. Son certificados de tipo Corporativo expedidos a entidades finales, personas vinculadas 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.

3. CERTIFICADO DE SERVIDOR SEGURO Son certificado que permiten identificar y vincular una determinada URL a una determinada entidad; un Colegio de Abogados, Consejo General de la Abogacía o Consejo Autonómico, así como cualquier persona jurídica vinculada al ejercicio profesional de la Abogacía."

4. CERTIFICADO RECONOCIDO DE PERSONA JURIDICA. Son certificados de tipo Corporativo expedidos a entidades finales, personas jurídicas que mantengan relación con los Colegios de Abogados o con la Abogacía Institucional.

5. CERTIFICADO RECONOCIDO DE PERSONA JURIDICA EN SOFTWARE
   Son certificados de tipo Corporativo expedido a Colegios de Abogados, Consejo General de la Abogacía y Consejos de Colegios de Abogados.

6. CERTIFICADOS RECONOCIDOS DE ABOGADO PENALNET: Son certificados de ámbito europeo y de tipo Corporativo expedidos a entidades finales, personas físicas pertenecientes a un asociación profesional, es decir, emitidos con la intervención de su asociación profesional en calidad de Registrador con la capacidad exclusiva de certificar la cualidad de "abogado" de una persona identificada en el certificado, de acuerdo con el Art 2 de la Directiva 98/5/EC (OJ No L 77 of 14 March 1998).

7. CERTIFICADOS RECONOCIDOS DE SELLO ELECTRÓNICO
   Son certificados de tipo Corporativo expedido a Colegios de Abogados, Consejo General de la Abogacía y Consejos de Colegios de Abogado y, en general, cualquier persona jurídica vinculada o relacionada de alguna forma con las profesiones

8. CERTIFICADOS RECONOCIDOS DE PERSONAL DE COLEGIO DE PROFESIONAL: Son certificados emitidos a entidades fínales, personas físicas vinculadas funcionalmente a un Consejo o Colegio profesional, que actúan como Registradores, o a instituciones vinculadas con estos.

9. CERTIFICADO RECONOCIDO DE ABOGADO EUROPEO
   Son certificados, de ámbito europeo y de tipo Corporativo expedidos a entidades finales, personas físicas pertenecientes a un Colegio de Abogados.

Los certificados reconocidos lo son de acuerdo con lo establecido en el art. 11 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, siendo obligatorio la utilización de un dispositivo criptográfico seguro que cumple las definiciones del art. 24 de la Ley de 59/2003 para la generación y custodia de los datos de creación de firma del suscriptor, y la creación de firmas, en esta misma línea le es de aplicación directa la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica, en aquellos puntos que no cubre la Ley 59/2003 de 19 de diciembre, de firma electrónica

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.

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_013.0
OID	1.3.6.1.4.1.16533.10.1.1
Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Versión:	013.0
Fecha de Emisión:	11/03/2014
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación.

1.3.1 Autoridad de Certificación (AC).

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

La 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 Declaración de Prácticas de Certificación (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 Consejo General de la Abogacía Española es el PSC en el ámbito de la emisión, publicación de certificados y listas de certificados revocados. AC Abogacía es la entidad emisora de los certificados de entidad final y responsable de las operaciones del ciclo de vida de los certificados, aunque para ciertas operaciones existan funciones delegadas en las Autoridades de Registro autorizadas.

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

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

1.3.4 Suscriptor

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

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

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

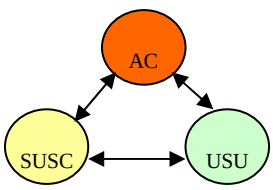
- Para los certificados de Personal Administrativo: personas pertenecientes a un Colegio o Consejo de Colegios de Abogados en calidad de empleados, colaboradores o vinculados a los mismos o a una entidad vinculada al mismo.

- Para Personas Jurídicas: tanto Colegios de Abogados como Consejos, o entidades vinculadas al entorno de la abogacía institucional

- Para los certificados europeos: las personas fisicas perteneciente a colegios de Abogados o a una asociación profesional en calidad de Abogado de acuerdo con el Art 2 de la Directiva 98/5/EC (OJ No L 77 of 14 March 1998)

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

Política de Certificado Reconocido de Colegiado (OID 1.3.6.1.4.1.16533.10.2.1)
Política de Certificado Reconocido de Personal Administrativo (OID 1.3.6.1.4.1.16533.10.3.1)
Política de Certificado de Servidor Seguro (OID 1.3.6.1.4.1.16533.10.4.1)
Política de Certificado Reconocido de Persona Jurídica (OID 1.3.6.1.4.1.16533.10.5.1)
Política de Certificado Reconocido de Persona Jurídica en software (OID 1.3.6.1.4.1.16533.20.2.1)
Política de Certificado Reconocido de Sello Electrónico (OID 1.3.6.1.4.1.16533.20.3.1)
Certificados Reconocidos de Abogado Penalnet (OID 1.3.6.1.4.1.16533.20.1.1)
Certificados Reconocidos de Personal de Colegio de Profesional (OID 1.3.6.1.4.1.16533.20.4.1)
Certificados Reconocidos de Abogado Europeo (OID 1.3.6.1.4.1.16533.10.9.1)

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 la CPS y las políticas de certificación específicas correspondientes.

No se permite el uso que sea contrario a la normativa española y comunitaria, a los convenios internacionales ratificados por el estado español, a las costumbres, a la moral y al orden público. Tampoco se permite la utilización distinta de lo establecido en las Políticas y en la Declaración de Practicas de Certificación.

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren

actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos.

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

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

La AC no crea, almacena ni posee en ningún momento la clave privada del suscriptor de certificados Reconocidos, no siendo posible recuperar los datos cifrados con la correspondiente clave pública en caso de pérdida o inutilización de la clave privada o del dispositivo que la custodia por parte del Suscriptor.

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

1.4. 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. 902 41 11 41
Fax	915327836
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 los artículos 18, 19 y 20 de la Ley 59/2003de 19 de diciembre, sobre firma electrónica, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 y otras normativas sobre prestación de servicios de certificación, así como lo dispuesto las Políticas de Certificación y en esta CPS. De forma especifica la AC se obliga a:

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

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

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:

- Abonar las tarifas establecidas por los servicios de certificación solicitados.
- Respetar lo dispuesto en esta CPS.
- Comprobar la identidad de los suscriptores y solicitantes de certificados.
- Verificar la exactitud y autenticidad de la información suministrada por el solicitante.
- Archivar, por periodo dispuesto en la legislación vigente, los documentos suministrados por el suscriptor.
- Respetar lo dispuesto en los contratos firmados con la AC.
- Respetar lo dispuesto en los contratos firmados con el Suscriptor.
- Informar a la AC las causas de revocación, siempre y cuando tomen conocimiento.

2.1.3 Solicitante

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

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

2.1.4 Suscriptor

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

- Custodiar su clave privada de manera diligente.
- Usar el certificado según lo establecido en la presente CPS y las Políticas de Certificación aplicables.
- Respetar lo dispuesto en los documentos firmados con la AR.
- Informar a la mayor brevedad posible de la existencia de alguna causa de suspensión /revocación.
- Notificar cualquier cambio en los datos aportados para la creación del certificado durante su periodo de validez.

- No utilizar la clave privada ni el certificado desde el momento en que se solicita o es advertido por la AC o la AR de la suspensión o revocación del mismo, o una vez expirado el plazo de validez del certificado.

2.1.5 Usuario

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

- Verificar la validez de los certificados en el momento de realizar cualquier operación basada en los mismos.
- Conocer y sujetarse a las garantías, límites y responsabilidades aplicables en la aceptación y uso de los certificados en los que confía.

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), o a través de otro canal que la AC considere seguro.

2.2. Responsabilidad

El Consejo General de la Abogacía Española (CGAE) ,en su actividad de prestación de servicios de certificación como CA, responderá por el incumplimiento de lo establecido en las Políticas y Prácticas de certificación y, allí donde sea aplicable, por lo que dispone la Ley 59/2003 de Firma Electrónica de 19 de Diciembre, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 o su normativa de desarrollo.

Sin perjuicio de lo anterior el Consejo General de la Abogacía Española no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en las Políticas y Prácticas de Certificación y en la Ley 59/2003, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 y su normativa de desarrollo, donde sea aplicable.

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 contenido de los mensajes o documentos firmados o encriptados digitalmente.

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

8. Fraude en la documentación presentada por el solicitante.

2.2.2 Límite de responsabilidad en caso de pérdidas por transacciones

El Consejo General de la Abogacía Española, en su actividad de Prestador de Servicios de Certificación como AC responderá de acuerdo con el régimen de responsabilidad que establece la Ley 59/2003, de Firma Electrónica, la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 y el resto de la legislación aplicable.

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

1. La exactitud de toda la información contenida en el certificado en la fecha de su emisión.

2. La garantía de que, en el momento de la entrega del certificado, obra en poder del Suscriptor, la clave privada correspondiente a la clave pública dada o identificada en el certificado.

3. La garantía de que la clave pública y privada funcionan conjunta y complementariamente.

4. La correspondencia entre el certificado solicitado y el certificado entregado

5. Cualquier responsabilidad que se establezca por la legislación vigente

2.3. Responsabilidad financiera

La AC en su actividad como Prestador de Servicios de Certificación 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.

La garantía citada se establece mediante un Seguro de Responsabilidad Civil con una cobertura igual o superior a 3.000.000 €.

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 y la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999.

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 Certificados

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

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

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.

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

2.6.2 Frecuencia de publicación

La publicación de las listas de los certificados revocados se ajustará a lo establecida en las Políticas de Certificación correspondientes.

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

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 direcciones URL contenidas en los propios certificado, en la extensión "*CRL Distribution Point*".

2.7. Auditorias

2.7.1 Frecuencia de las auditorías

Se realiza una auditoria con carácter periódico.

2.7.2 Identificación y calificación del auditor

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

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

2.7.3 Relación entre el auditor y la AC

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

2.7.4 Tópicos cubiertos por la auditoria

La auditoria verifica los siguientes principios:

- Publicación de la Información: Que la AC hace públicas las Prácticas de Negocio y de Gestión de Certificados (Políticas y CPS), así como la protección de datos personales y proporciona sus servicios en conformidad con dichas afirmaciones.
- Integridad de Servicio. Que la AC mantiene controles efectivos para asegurar razonablemente que:
    a. La información del suscriptor es autenticada adecuadamente (para las actividades de registro realizadas por la AC).
    b. La integridad de las claves y certificados gestionados y su protección a lo largo de todo su ciclo de vida.
- Controles generales. Que la AC mantiene controles efectivos para asegurar razonablemente que:
    a. 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.
    b. Se mantiene la continuidad de las operaciones relativas a la gestión del ciclo de vida de las claves y los certificados.
    c. 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 podrán ser auditadas previamente a su puesta en marcha efectiva. Adicionalmente, se podrán realizan auditorias periódicas que comprueban el cumplimiento de los requerimientos exigidos por las políticas de certificación para el desarrollo de las labores de registro expuestas en el contrato de servicio firmado.

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 y Protección de Datos Personales

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

La AC cumple 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.

Según lo dispuesto en el artículo 19.3 de la ley 59 /2003 de Firma electrónica, esta CPS deberá considerarse el "Documento de Seguridad" a los efectos previstos en la legislación sobre protección de datos y su desarrollo normativo.

2.8.1 Tipo de información a mantener confidencial

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

2.8.2 Tipo de información considerada no confidencial

La siguiente información será considerada no confidencial:

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

- Cualquier información cuya publicidad sea impuesta normativamente.

2.8.3 Divulgación de información de revocación / suspensión de certificados

La AC 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.

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.

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.

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

3.1.2 Pseudónimos

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

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. La AC no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

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

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

La AC en todo caso se atiene a lo dispuesto en el apartado 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.

3.1.8 Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del suscriptor de certificados personales, la AC exige la personación física del suscriptor ,

En el caso del certificado de Persona Jurídica se exigirá la personación del Representante ante la AR y la presentación del Documento Nacional de Identidad, pasaporte Español o Tarjeta de Extranjero ante un operador o personal debidamente autorizado de la Autoridad de Registro.

En el caso de los certificados de servidor seguro no será necesaria la personación del solicitante ante la AR

En el caso de la emisión de certificados europeos se exigirá la personación del suscriptor y la identificación por cualquiera de los medios que la Autoridad de Registro considere valido para el proceso.

En caso que el titular reclame la modificación de los datos de identificación personales a registrar respecto de los del DNI, deberá presentar el correspondiente Certificado del Registro Civil consignando la variación.

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 certificados emitidos con posterioridad a la entrada en vigor de la Ley 59/2003 de Firma Electrónica, 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

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.

La renovación se notificará al suscriptor con suficiente antelación antes de que su certificado vaya a caducar para que pueda proceder a su renovación.

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

La emisión de los certificados se regirá según lo dispuesto en cada Política de Certificación

4.2. Emisión de certificados

El proceso seguido para la emisión de certificados se establecerá en cada Política de Certificación

4.3. 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.

La suspensión y revocación de certificados serán notificadas al suscriptor del certificado mediante un correo electrónico a la cuenta de correo que figura en el certificado suspendido o revocado.

4.3.1 Causas de revocación de certificados

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

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

   - Modificación de alguno de los datos contenidos en el certificado.
   - Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.
   - Pérdida o cambio del suscriptor de la vinculación con la institución, en el caso de Certificados de Personal Administrativo

   Esta causa de revocación podrá solicitarla el usuario a través del código de revocación o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

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

- Compromiso de la clave privada o de la infraestructura o sistemas 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.

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

Las causas de revocación relativas a certificados de usuarios podrá solicitarla el usuario a través del código de revocación o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

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 de la clave privada.

- 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.

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

Las causas de revocación relativas a certificados de usuarios podrá solicitarla el usuario a través del código de revocación o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas.

4. Circunstancias que afectan al suscriptor

- Manifestación expresa y univoca del suscriptor o tercero autorizado

- Finalización de la relación jurídica entre la AC, la AR y el Suscriptor.

- Modificación o extinción de la relación jurídica subyacente o causa que permitió la emisión del certificado al suscriptor, incluyendo la inhabilitación temporal del colegiado para el ejercicio profesional.

- Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

- Infracción por el suscriptor, de sus obligaciones, responsabilidad y garantías, establecidas en el instrumento jurídico correspondiente o en la CPS de la AC.

- La incapacidad sobrevenida, total o parcial.

- Por el fallecimiento del suscriptor.

Las causas de revocación relativas a certificados de usuarios podrá solicitarla el usuario a través del código de revocación o el Operador de la AR, siempre que existan dudas fundadas de alguna de las causas expuestas

5. Otras circunstancias

- La suspensión del certificado digital por un período superior al establecido en la CPS.

- Por resolución judicial o administrativa que lo ordene.

- Por la concurrencia de cualquier otra causa especificada en la CPS.

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

Si la AR 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. Cuando el suscriptor tenga conocimiento de la suspensión del certificado deberá abstenerse de utilizarlo, y contactar con la AR o la AC para proceder a su revocación o al levantamiento de la suspensión, su hubiere lugar.

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

4.3.2 Quién puede solicitar la revocación

Pueden solicitar la 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 siempre que tenga motivos fundados

- Los Administradores autorizados de la AC siempre que tenga motivos fundados.

4.3.3 Procedimiento de solicitud de revocación

El procedimiento de solicitud de revocaciones o suspensiones presenta puede iniciarse por vía presencial, 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, su deseo de revocar suspender o revocar el certificado. El operador procederá a efectuar la suspensión o revocación, informando al suscriptor de la realización del trámite.

- Suspender por parte de un tercero: En el caso de ser un tercero el que manifiesta la solicitud, el operador le realizará una seria de preguntas para determinar la causa de la solicitud, recibirá la documentación pertinente, y si considera que concurren las causas establecidas procederá a efectuar la suspensión, una suspensión cautelar a la espera de más averiguaciones. Asimismo, enviará un mensaje al suscriptor comunicándole la circunstancia.

Procedimiento online:

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

- Acceder a http://www.acabogacia.org
- Seleccionar: Zona usuarios → Gestión de certificados → Revocación On-line
- Introducir el Código de Revocación proporcionado durante el proceso de generación del certificado.

El sistema el certificado. Al tiempo de revocarse el certificado, se notificará al suscriptor, comunicando la hora de revocación y la causa de la misma.

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.

4.3.4 Periodo de revocación

Sin estipulación

4.3.5 Suspensión

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

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

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

Si la AR 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).

4.3.6 Quién puede solicitar la suspensión

Pueden solicitar la suspensión de un certificado:

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

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

4.3.7 Procedimiento para la solicitud de suspensión

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

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

4.3.8 Límites del periodo de suspensión

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

4.3.9 Frecuencia de emisión de CRL's

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

La AC ACA Certificados Corporativos emitirá una nueva CRL cada vez que esta una modificación del estado de un certificado de su jerarquia

La AC ACA Trusted emitirá una nueva CRL cada vez que esta una modificación del estado de un certificado de su jerarquia

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

Los certificados revocados que expiren son retirados de la CRL.

La AC mantendrá un histórico de CRl´s y ARl´s emitidas.

4.3.10 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 las direcciones URL contenidas en el propio certificado, en la extensión "*CRL Distribution Point*".

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

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

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

4.3.11 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.

4.3.12 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 asociado al certificado que desea verificar.

4.3.13 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.

4.3.14 Otras formas de divulgación de información de revocación disponibles

Sin estipulación

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

Sin estipulación

4.3.16 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.

4.4. Procedimientos de Control de Seguridad

4.4.1 Tipos de eventos registrados

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

- 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 AC.
- Registros de la destrucción de los medios que contienen las claves, datos de activación.

Adicionalmente la AC conserva, ya sea manual o electrónicamente, la siguiente información:

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

4.4.2 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.

4.4.3 Periodos de retención para los Logs de auditoría

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

4.4.4 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.

4.4.5 Procedimientos de backup de los Logs de auditoría

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

La AC tiene implementado un procedimiento de back up seguro de los logs de auditoría, realizando 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.

4.4.6 Sistema de recogida de información de auditoria

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

4.4.7 Notificación al sujeto causa del evento

No estipulado.

4.4.8 Análisis de vulnerabilidades

La AC 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.
Archivo de registros

4.4.9 Tipo de eventos registrados

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

- 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.

4.4.10 Periodo de retención para el archivo

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

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

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

4.4.12 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.

Los BackUps estan firmados para garantizar su integridad

4.4.13 Requerimientos para el sellado de tiempo de los registros

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

Relación de servidores de sincronización del servidor de Acabogacia.

hora.roa.es stratum 1
ntp.dgf.uchile.cl
time.xmission.com
clock.via.net
time.keneli.org

La sincronización

Al arrancar el demonio ntpd el sistema lee de los ficheros de configuración, entre otros.

Las direcciones IP o los nombres de los servidores de referencia
El máximo y el mínimo intervalo de tiempo transcurrido entre dos consultas a esos servidores

La corrección del reloj interno

Utilizando la lista de servidores, se solicita información horaria de todos ellos. En esta información, además de la hora, llegan datos acerca del retardo del paquete en su viaje por la red, de la estabilidad y de calidad de los servidores.

Al mismo tiempo, si el sistema ya ha corrido ntpd durante un tiempo suficiente en una sesión anterior, lee la última corrección que hay que hacer a la frecuencia interna del reloj para mantener la hora correcta en un margen adecuado.

El servidor de hora calcula su hora contando los ciclos que completa determinados osciladores. A éstos se les supone una frecuencia que puede que no sea la correcta. NTP es capaz de estimar su error e imponer al Kernel que tenga en cuenta esa corrección.

Conforme el tiempo avanza, las correcciones que ntpd hace son más fiables, el sistema es mas estable y el intervalo transcurrido entre dos consultas al servidor de tiempos va aumentando. El error máximo que se le permite al reloj del sistema es de 128 milisegundos.

Si se supera este límite, el sistema se declara de nuevo no sincronizado y todo comienza como desde el arranque. No suele ocurrir eso, el servidor de tiempo a las dos horas tiene un error del orden de 2 milisegundos

4.4.14 Sistema de recogida de información de auditoria

No estipulado.

4.4.15 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.

4.5. Cambio de clave

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

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

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

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

4.6.1 La clave de una entidad se compromete

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

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

- Informará a todos los suscriptores, usuarios y otras CA's con los cuales tenga acuerdos u otro tipo de relación del compromiso, como mínimo mediante la publicación de un aviso en la página web de la AC.
- Indicará que los certificados e información relativa al estado de la revocación firmados usando esta clave no son válidos.

4.6.2 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.

4.7. 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 hasta el cese definitivo de la actividad, si es el caso.
- Informará a todos los suscriptores, solicitantes, usuarios, otras CA's o entidades con los cuales tenga acuerdos u otro tipo de relación del cese con la anticipación mínima de 2 meses, o el periodo que establezca la legislación vigente.

- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- De acuerdo con el artículo 21 de la Ley 59/2003 de Firma Electrónica, la AC podrá transferir, con el consentimiento expreso de los suscriptores, la gestión de los certificados que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La AC informará, cuando sea el caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.
- Informará a la administración competente, con la antelación indicada, el cese de su actividad y el destino que se vaya a dar a los certificados, especificando, en su caso, si se va a transferir la gestión y a quién.
- Con carácter previo al cese definitivo de la actividad, comunicará a la administración competente la información relativa a los certificados reconocidos expedidos al público cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f) de la Ley 59/2003 y la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999 por la que se establece un marco común para la firma electrónica,

5. Controles de Seguridad Física, Procedimental y de Personal

5.1. Controles de Seguridad física

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

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

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

Las instalaciones cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

Ubicación y construcción

Las instalaciones están localizadas en zona industrial, en el norte del área metropolitana de Madrid, junto a una de las principales áreas de negocios, a 15 minutos de la zona centro de un Madrid y a 15 minutos del aeropuerto de Madrid - Barajas. El acceso a nudo de autopistas y circunvalaciones (M-30,M-40) está a unos 500 metros del edificio

El edificio del CPD se encuentra recogido en el Plan de Emergencia Civil Nacional del Ministerio de Ciencia y Tecnología dado el alto valor de las comunicaciones y clientes alojados en el edificio.

5.1.1 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 doble filmación por circuito cerrado de televisión y su archivo.

Las instalaciones cuentan con personal privado de seguridad.

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

5.1.2 Alimentación eléctrica y aire acondicionado

El centro dispone de un sistema de alimentación de corriente alterna, filtrada y balanceada a través de dos UPS en redundancia n+1, que permiten una potencia desde 400 hasta 2.000 W/m2, y una capacidad de 7,5 a 25 MW sin punto único de fallo. En los racks de los sistemas existen dos tomas eléctricas, redundantes e independientes: UPS1 y UPS2, distribuidas a través de blindobarras de cobre que permiten una mejor y mayor capacidad de distribución eléctrica al edificio. Adicionalmente existen generadores diesel en redundancia n+1 con una autonomía de 48 horas y un contrato con el distribuidor de gasoil que garantiza la recarga de los tanques en un tiempo inferior a 4 horas.

El centro dispone de Sistemas de Control de Temperatura y Humedad (HVAC). El sistema HVAC está basado en la gestión del ambiente mediante el enfriamiento de agua y permite un control constante de temperatura de 21ºC +/- 5ºC con una humedad relativa del 20% al 80%. Las bombas y los refrigeradores están situados en la planta superior con redundancia n+1 y sin ningún punto único de fallo. Del mismo modo, la distribución del mismo sobre el edificio mantiene la redundancia en anillos con sensores ante detección de fugas. En cada sala existe un sistema igualmente redundado de aire acondicionado y filtrado

5.1.3 Exposición al agua

Las instalaciones de AC están ubicadas en una zona de bajo riesgo de inundación.

5.1.4 Protección y prevención de incendios

Protección de incendios. El sistema de detección de incendios consta de múltiples sensores ópticos situados en techo y suelo de cada una de las salas técnicas. El sistema entra en funcionamiento en el momento que más de dos detectores de humo se activan y es completamente direccionable para el edificio entero, permitiendo la detección cruzada (en techo y en piso elevado) El sistema de extinción permite el disparo automático y manual y está basado en la inundación total de la sala con gas F-13, que es almacenado en cuartos separados en el edificio.

5.1.5 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.

5.1.6 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.

5.1.7 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.

Según lo especificado en la norma CEN CWA 14167-1, los roles mínimos establecidos son:

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

Concretamente:

Las tareas de Auditor son incompatibles en el tiempo con las tareas de Certificación e incompatibles con 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 de una sola persona autorizada.

- Revisión de logs a excepción de los de la CA
- Reinicio de servicios a excepción de los de CA
- Vision de grabaciones del CCTV

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

- La activación de la clave privada de las CA's para la emisión de certificados de las CA's
- La activación de la clave privada de las CA's para el cambio o creación de nuevos perfiles de certificación
- La activación de la clave privada de las CA root para la emisión de ARLs
- Revisión de logs de la CA.
- Instalación o actualización de software de certificación
- Configuración de software de certificación

Las siguientes tareas requerirán al menos un control de tres personas o mas confiables:

- La generación de claves de CA.
- La recuperación del back-up de la clave privada de las CA's.
- La generación de nuevos Set de Tarjetas de Operador

- La eliminación de un Set de Tarjetas de Operadores

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 cuatro meses trabajando en el centro de producción.

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

La AC se asegura que el personal de registro es personal confiable de un Colegio o del organismo delegado para realizar las tareas de registro. A tal efecto se exige una declaración en tal sentido por parte de la Entidad que asume funciones de AR.

El empleado del registro habrá realizado un curso de preparación para la realización de las tareas de registro y validación de las peticiones. Al final de dicho curso, un auditor externo procederá a evaluar sus conocimientos del proceso.

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

La AC realiza las investigaciones pertinentes antes de la contratación de cualquier persona. La AC nunca asigna tareas confiables a personal con una antigüedad inferior a cuatro meses. Las AR pueden establecer criterios diferentes, siempre que lo soliciten y la AC tras estudiar el caso lo apruebe.

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

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

5.3.5 Frecuencia y secuencia de rotación de tareas

No estipulado.

5.3.6 Sanciones por acciones no autorizadas

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

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 a sanciones.

5.3.8 Documentación proporcionada al personal

La AC pondrá a disposición de todo el personal la documentación donde se detallen las funciones encomendadas Las políticas y 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 AC 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

En las Políticas de Colegiado y Personal Administrativo, Las claves de los suscriptores y operadores son generadas por el propio interesado de forma segura utilizando un dispositivo criptográfico CC EAL4+, FIPS 140-1 nivel 2, 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, con los adecuados parámetros. Las claves tienen una longitud mínima de 2048 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 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/doc

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

Jerarquía de Certificación en vigor desde el 05/03/2014	
CA Raíz	SHA-1: 7F8A 7783 6BDC 6D06 8F8B 0737 FCC5 7254 1306 8CA4
CA ACA Corporativos 2014	C0 B0 E5 A1 28 D1 4D 73 C1 61 28 B2 C5 47 92 95 F7 E4 A1 20
CA ACA-Trusted 2014	E6 A4 B6 E4 D7 4A 0F 70 C3 57 8A C6 53 12 B5 03 84 FC BF 3D

Jerarquía de Certificación desde el 01/07/2005	
CA Raíz	SHA-1: 7F8A 7783 6BDC 6D06 8F8B 0737 FCC5 7254 1306 8CA4
CA ACA Corporativos	SHA-1: 67B8 6CDB DEFD 4A8D F14A 6C14 46B1 EE04 3807 CB9B
CA ACA-Trusted (vigente desde 02/06/2009)	SHA-1: AC CF FC 6A 97 A9 73 DF F7 DB EE DE 58 D6 E9 3C B3 20 53 98

Jerarquía de Certificación previa al 01/07/2005	
CA Raíz	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
Certificados emitidos antes de 02/03/2004	
CA Corporativos	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
Certificados emitidos entre 02/03/2004 y el 01/07/2005	
CA Corporativos	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

Los usuarios pueden solicitar la reemisión de una copia autenticada en papel de los datos anteriores en las 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

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

El periodo de uso de la clave privada de la CA Raíz es de 25 años. El periodo de uso de la clave privada de la CA de AC Abogacía es de 12 años. Las fechas concretas pueden obtenerse de los propios certificados de CA.

La CA Raíz dejará de emitir certificados 12 años antes de expiración de su periodo de validez, la CA de AC Abogacía dejará de emitir certificados 3 años antes de la expiración de su periodo de validez

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 mínima de 2048 bits.

El periodo de uso de la clave pública y privada del suscriptor corresponde con la validez temporal de los certificados que se establecerá en cada Política de Certificación, 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

Según lo dispuesto en las Políticas de Certificación (CP). Consulte http://www.acabogacia.org/doc.

Las claves de las CA's vinculadas son generadas en un modulo criptográfico validado FIPS140-1 nivel 3

6.1.8 Fines del uso de la clave

La AC Raíz y la AC intermedia incluirán las siguientes extensiones dentro de sus certificados:

keyUsage = (critica) keyCertSign, cRLSign
netscapeCertType = SSL_CA, SMIME_CA, ObjectSigning_CA

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 cinco 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 es mantenida y usada en un dispositivo criptográfico seguro que cumple los requerimientos que se detallan en el FIPS 140-1 nivel 3.

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

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

Clave privada del suscriptor

La clave privada del suscriptor, es controlada y gestionada por el suscriptor. Tiene un sistema de protección contra intentos de acceso.

6.3. Estándares para los módulos criptográficos

Los módulos criptográficos empleados en la CA emisora a entidades finales 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 cinco 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 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 dispone de Back up que permite la reconstrucción de la clave privada de la CA en caso de perdida de esta y 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

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

La CA no hace custodia de claves privadas de usuario.

6.3.5 Introducción de la clave privada en el módulo criptográfico

Existe un documento de ceremonia de claves de 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

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

Según lo dispuesto en las Políticas de Certificación.

6.3.8 Método de destrucción de la clave privada

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

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

6.4.2 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 en línea 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)

Según lo dispuesto en las Políticas de Certificación (CP). Consulte http://www.acabogacia.org/doc.

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 en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de Usuarios y permisos.
- Configuración de eventos de log.
- Plan de backup y recuperación.
- Requerimientos de tráfico de red.

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

6.6.1 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 está garantizada por las instalaciones ya definidas anteriormente y la gestión de personal.

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 Cortafuegos 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.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 está 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

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 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

7.1.1 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 conocida como"*European profile for Qualified Certificates"* y las RFC[2] 3039 (substituída) y 3739 "*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 art. 11 de la Ley 59/2003, con el contenido prescrito por el art. 11 de la Ley 59/2003, y expedidos en un dispositivo que sigue las definiciones del art. 24 de la Ley 59/2003. Los certificados que corresponden a certificados reconocidos lo son de acuerdo con lo definido en los apartados 5.2 y 5.3 de la especificación técnica TS 101 456 del Instituto Europeo de Normas de Telecomunicaciones (ETSI).

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 RFC3280 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.

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

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

[1] Ver párrafo "Aclaraciones sobre la extensión X509v3 KeyUsage"
[2] Ídem

7.1.2 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 = ACA - Certificados Corporativos OU = Autoridad de Certificacion de la Abogacia O = Consejo General de la Abogacia NIF:Q-2863006I E = ac@acabogacia.org L = Madrid 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**)

7.1.3 Número de versión

La AC emite certificados X.509 Versión 3.

7.1.4 Extensiones del certificado

Se aplicará lo establecidos en cada PC.

7.1.5 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

7.1.6 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.

7.2.1 Número de versión

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

7.2.2 CRL y extensiones

Se aplicará lo establecido en cada PC

8. ESPECIFICACIÓN DE LA ADMINISTRACIÓN

8.1. Autoridad de las políticas

El departamento de operaciones de AC Abogacía es responsable de la administración de las CPS. Puede contactar en:

Persona de contacto:
Administrador AC Abogacía
Departamento de Operaciones

E-mail:	info@acabogacia.org
Teléfono:	Tel. 902 41 11 41
Dirección:	Consejo General de la Abogacía Española Paseo de Recoletos, 13 28004 Madrid

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. Las versiones anteriores podrán ser retiradas de su consulta on-line, pero pueden ser solicitadas por los interesados en AC Abogacía.

Los usuarios pueden solicitar una copia de 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, después de comprobar el cumplimiento de los requisitos establecidos por el Consejo General de la Abogacía Española.

Anexo 1: Documento de Seguridad (LOPD)

PREAMBULO

El Consejo General de la Abogacía Española protegerá los ficheros con datos de carácter personal necesarios para realizar la actividad de prestación de servicios de certificación digital de acuerdo con lo previsto en la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el Reglamento de medidas de seguridad aprobado por el Real Decreto 994/1999, de 6 de junio (RD 994/1999) y demás normativa aplicable. Dichos Ficheros serán de titularidad privada y su creación, modificación o supresión se notifica a la Agencia Española de Protección de Datos mediante los mecanismos habilitados al efecto.

Para la prestación efectiva del servicio, es necesario que los suscriptores faciliten en su totalidad y con información verdadera los datos necesarios para la emisión de los certificados. Dichos datos son recogidos con esa finalidad, y el solicitante, futuro suscriptor, consiente el tratamiento de los mismos para los usos y finalidades establecidos. Según lo especificado en el citado Reglamento, los datos personales contenidos en los ficheros corresponden al nivel básico.

Para realizar la actividad de PSC propia y el correcto funcionamiento del servicio, diferentes entidades externas deben tener acceso a los datos, en particular las Autoridades de Registro, así como diversos proveedores que colaboran para la prestación del servicio. El Consejo General de la Abogacía Española será, en cualquier caso, el Responsable del Fichero, quedando estas entidades como Encargadas del Tratamiento, exclusivamente para los fines que figuran en la CPS, y comprometiéndose a tratar los mismos siguiendo las instrucciones de el Consejo General de la Abogacía Española, no comunicarlos a terceros y destruir o devolverlos una vez que su relación con el Consejo General de la Abogacía Española finaliza, salvo aquellos que deban ser conservados según lo establecido en la legislación vigente sobre Firma Electrónica.

Los Usuarios (terceros que confían en los certificados) pueden consultar los datos contenidos en los certificados así como el estado de vigencia o validez en el directorio de certificados, de acceso público según lo establecido en la Ley 59/2003 de Firma Electrónica. Los Usuarios únicamente podrán utilizar la información para la verificación de la validez del certificado o de las firmas generadas de acuerdo con lo establecido en la legislación vigente, la CPS y las Políticas de Certificación. Se advierte, con carácter general, que cualquier tratamiento, registro o utilización para otros fines distintos de los anteriores requiere obligatoriamente del consentimiento previo de los titulares de los datos. Se advierte que la LOPD sanciona con multas que pueden alcanzar los SEISCIENTOS MIL EUROS (600.000€) por cada una de las infracciones o incumplimientos de dicha Ley, sin perjuicio de la incoación de acciones penales de acuerdo con el Código Penal, así como de reclamaciones civiles de los perjudicados.

Los titulares de los datos podrán ejercer los derechos de acceso, rectificación, cancelación y oposición frente al Consejo General de la Abogacía Española, en la dirección que se indica en http://www.cgae.es indicando como referencia en la comunicación “DATOS

PERSONALES", sin perjuicio de las obligaciones de conservación de determinados datos que establece la ley 59/2003 de Firma Electrónica.

A. AMBITO DE APLICACIÓN DEL DOCUMENTO DE SEGURIDAD

El presente documento, parte integrante de la CPS de AC Abogacía, tiene como finalidad establecer las medidas técnicas y organizativas necesarias para garantizar la seguridad que deben reunir los ficheros automatizados, locales, equipos, sistemas y las personas que intervengan en el tratamiento automatizado de los datos de carácter personal.

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

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

La CPS, de la cual forma parte este Documento de Seguridad es de obligado cumplimiento para todo el personal de la institución. Las normas internas contenidas en el presente documento se han puesto en conocimiento de todo el personal de la institución, con el objeto de dar debido cumplimiento a la obligación contenida en el art. 9.2 del Real Decreto 994/1999, de 11 de junio.

B. FUNCIONES Y OBLIGACIONES DEL PERSONAL

En relación con el uso y tratamiento de datos personales, el Consejo General de la Abogacía Española establece dos funciones diferenciadas:

Responsable del Fichero. El responsable del fichero, que puede delegar alguna de las tareas en el responsable de seguridad, tiene las siguientes funciones:

1. Notificar a la Agencia de Protección de Datos los ficheros de datos personales de el Consejo General de la Abogacía Española
2. Velar por el cumplimiento de todos los requisitos establecidos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter Personal y en el Real Decreto 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de Seguridad de los ficheros automatizados que contengan datos de carácter personal y por el cumplimiento de las normas de seguridad contenidas en el documento de seguridad.
3. Redactar, establecer y comprobar la aplicación y el cumplimiento del documento de seguridad.
4. Establecer los criterios que el responsable de seguridad debe seguir al realizar la función de conceder, alterar o anular el acceso autorizado a los datos y recursos.
5. Establecer los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.
6. Mantener actualizado el registro de incidencias.

7. Autorizar la salida de soportes que contengan datos de carácter personal.
8. Nombrar uno o varios responsables de seguridad, encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero.
9. Adoptar las medidas correctoras adecuadas, en función del análisis de los informes de auditoría realizado por el responsable de seguridad.

Responsable de Seguridad. El responsable de seguridad tiene encomendadas las siguientes funciones:

1. Velar por el cumplimiento de las normas de seguridad contenidas en el documento de seguridad.
2. Recopilar y describir las medidas, normas, procedimientos, reglas y estándares de seguridad adoptados por el Consejo General de la Abogacía Española.
3. Determinar y describir los recursos informáticos a los que se aplicará el documento de seguridad.
4. Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
5. Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos.
6. Comprobar el cumplimiento de la periodicidad establecida para la realización de copias de respaldo.
7. Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al sistema informático del Consejo General de la Abogacía Española., con especificación del nivel de acceso que tiene cada usuario.
8. Establecer y comprobar la aplicación del procedimiento de identificación y autenticación de usuarios.
9. Establecer y comprobar la aplicación del procedimiento de asignación, distribución y almacenamiento de contraseñas.
10. Comprobar, en la medida de lo posible, el mantenimiento de la confidencialidad de las contraseñas de los usuarios.
11. Establecer y comprobar la aplicación del procedimiento de cambio periódico de las contraseñas de los usuarios.
12. Establecer y comprobar la aplicación de un procedimiento que garantice el almacenamiento de las contraseñas vigentes de forma ininteligible.
13. Establecer y comprobar la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
14. Establecer y comprobar los mecanismos que faciliten al usuario el acceso a datos o recursos a los que está autorizado.
15. Conceder, alterar o anular el acceso autorizados a los datos y recursos, de acuerdo

con los criterios establecidos por el responsable del fichero.

16. Establecer y comprobar la aplicación de un sistema que permita identificar, inventariar y almacenar en lugar seguro los soportes informáticos que contienen datos de carácter personal.
17. Velar por el cumplimiento de las normas de seguridad, comunicando al responsable del fichero las infracciones cometidas, que podrían ser sancionables según las normas laborales de aplicación.
18. Establecer y comprobar la aplicación de controles periódicos para verificar el cumplimiento de lo dispuesto en el documento de seguridad.
19. Establecer y comprobar la aplicación de las medidas de seguridad que se deban adoptar cuando un soporte vaya a ser desechado o reutilizado.
20. Coordinar y controlar las medidas definidas en el documento de seguridad.
21. Coordinar y controlar la realización de una auditoría interna o externa sobre los sistemas de información e instalaciones en los que se lleva a cabo el tratamiento de los datos personales, que verifique el cumplimiento del Reglamento de Seguridad y de los procedimientos e instrucciones vigentes en materia de seguridad de datos.
22. Establecer y comprobar la aplicación de medidas de control del acceso físico a los locales donde se encuentre ubicado los sistemas de información con datos de carácter personal.
23. Establecer y comprobar la aplicación de un registro de entrada de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.
24. Establecer y comprobar la aplicación de un registro de salida de soportes informáticos que permita, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el destinatario, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la entrega que deberá estar debidamente autorizada.
25. Establecer y comprobar la aplicación de las medidas necesarias para impedir la recuperación posterior de la información almacenada en los soportes informáticos que van a ser desechados o reutilizados.
26. Establecer y comprobar la aplicación de las medidas necesarias para impedir la recuperación indebida de la información almacenada en los soportes informáticos que vayan a salir fuera de los locales en que se encuentran ubicados los ficheros.
27. Hacer el seguimiento del registro de incidencias y ampliar los campos del mismo para dejar constancia de los procedimientos realizados para la recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.
28. Autorizar por escrito la ejecución de los procedimientos de recuperación de datos.
29. Comprobar que en la fase de pruebas de los sistemas de información, éstas no se efectúen con datos personales reales.
30. Publicar las normas internas.

31. Revisar el conocimiento de las normas internas por parte del personal de la empresa.
32. Velar por el cumplimiento de las normas internas del Consejo General de la Abogacía Española.

En relación con la gestión y operación de la actividad de Prestación de Servicios de Certificación, se establecen otros roles y funciones según lo establecido en las normas CEN CWA 14167-1, y que se detallan en el apartado 5.2.1.

C. ESTRUCTURA DE LOS FICHEROS Y DESCRIPCIÓN DE LOS SISTEMAS QUE LOS TRATAN

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

Datos de Identificación:

- Nombre, Apellidos y NIF

Datos de contacto:

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

Datos profesionales:

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

Datos del certificado de clave digital de clave pública:

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

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

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

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

D. MEDIDAS PARA GARANTIZAR EL NIVEL DE SEGURIDAD

Las medidas implantadas para garantizar los niveles de seguridad exigibles por el Reglamento de Protección de Datos, en su nivel básico, son ampliamente superadas por las exigencias legales y de buenas prácticas a implantar para prestar servicios de Certificación. Las medidas específicas asociadas al sistema de certificación, que trata los ficheros con datos personales, se describen en los capítulos 4, 5 y 6 de esta CPS.

Control interno y auditoría

De forma continuada y con una frecuencia mínima de una vez al año, se llevarán a cabo los controles periódicos que se deben realizar para verificar el cumplimiento de lo dispuesto en el documento de seguridad.

Los controles periódicos actuarán en las siguientes áreas:

- Control de la aplicación del plan de seguridad
- Control del sistema de identificación y autenticación
- Control del sistema de control de acceso
- Control del cumplimiento de las normas de confidencialidad y secreto
- Control del cumplimiento de las normas internas y las funciones del personal
- Control antivirus
- Control del cumplimiento de las normas de propiedad intelectual

Los datos incluidos en los ficheros se caracterizan como de nivel básico, por lo que es no es obligatoria la realización de auditorías externas específicas. Sin embargo, los procedimientos y medidas de seguridad son auditados en el marco de la Auditoría voluntaria de la actividad de Prestación de Servicios de Certificación, como se establece en el apartado 2.7.

Adicionalmente, el Consejo General de la Abogacía Española establece las siguientes Medidas Generales de Seguridad, que afectan a todos los sistemas, equipos, usuarios y procedimientos, aunque no estén implicados directamente en el tratamiento de datos personales.

Medidas Generales de Seguridad

D.1 Identificación y autenticación

1. Existe una relación actualizada de usuarios que tienen acceso autorizado a los sistemas de información.
2. El responsable de seguridad custodiará y actualizará la relación de todos los usuarios de la red que tienen acceso autorizado a los sistemas de información. Es competencia del responsable de seguridad que la atribución y asignación de contraseñas, así como la custodia de la relación de usuarios se realice de forma que se garantice su confidencialidad e integridad.
3. Existe un procedimiento de identificación y autenticación de los usuarios que deseen acceder al sistema. Los usuarios se identifican en el sistema mediante su nombre de usuario y su clave de acceso, o mediante el correspondiente certificado digital. Igualmente, existe un procedimiento de asignación, distribución y almacenamiento de contraseñas que garantiza su confidencialidad e integridad.
4. Los números de identificación y claves de acceso asignadas a cada usuario de la red corporativa del Consejo General de la Abogacía Española. son personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de los mismos.
5. Las contraseñas de los usuarios autorizados tendrán una longitud mínima de cuatro caracteres. Durante el tiempo que estén vigentes, las contraseñas se almacenarán de forma ininteligible.
6. El responsable de seguridad establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder al sistema de información y la verificación de que está autorizado.

D.2 Control de acceso y confidencialidad de la información

1. Toda la información albergada en la red corporativa del Consejo General de la Abogacía Española o de sus proveedores, de forma estática o circulando en forma de mensajes de correo electrónico, es propiedad del Consejo General de la Abogacía Española. y tiene el carácter de confidencial respecto de terceros externos a Consejo General de la Abogacía Española.
2. Tendrán el carácter de información especialmente reservada los secretos industriales o comerciales de la empresa, en los que se incluyen, sin carácter limitativo, los procedimientos, metodologías, código fuente, algoritmos, bases de datos de carácter personal (datos de clientes, proveedores, etc.), planes de marketing, y cualquier otro material que forma parte de la estrategia industrial o comercial del Consejo General de la Abogacía Española.
3. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. En especial, el sistema de certificación dispondrá de separación de roles y privilegios según lo recogido en el apartado correspondiente de la CPS.
4. Para acceder a los locales donde se encuentre el sistema de certificación de Consejo General de la Abogacía Española se deberá pasar por un sistema de control de acceso físico, que impida el acceso de personal no autorizado.
5. Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

D.3 Uso del correo electrónico

2. El sistema informático, la red corporativa y los terminales utilizados por cada usuario son propiedad del Consejo General de la Abogacía Española o de sus proveedores en los casos en que el servicio se ha establecido así.
3. Ningún mensaje de correo electrónico será considerado como privado. Se considerará correo electrónico tanto el interno, entre terminales de la red corporativa, como el externo, dirigido o proveniente de otras redes públicas o privadas, y, especialmente, Internet.
4. El Consejo General de la Abogacía Española se reserva el derecho de revisar por ella misma o mediante la prestación de servicios de un tercero, sin previo aviso, los mensajes de correo electrónico de los usuarios de la red corporativa y los archivos LOG del servidor de correo, con el fin de comprobar el cumplimiento de estas normas y prevenir actividades que puedan afectar al Consejo General de la Abogacía Española como responsable civil subsidiario.
5. Cualquier fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

D.4 Acceso a Internet

1. El uso del sistema informático del Consejo General de la Abogacía Española para acceder a redes públicas como Internet, se limitará a los temas directamente relacionados con la actividad del Consejo General de la Abogacía Española y los cometidos del puesto de trabajo del usuario.
2. El acceso a debates en tiempo real (Chat / IRC) es especialmente peligroso, ya que facilita la instalación de utilidades que permiten accesos no autorizados al sistema, por lo que su uso queda estrictamente prohibido. Todo ello, salvo que medie autorización expresa del responsable de seguridad.
3. El acceso a páginas web (WWW), grupos de noticias (Newsgroups) y otras fuentes de información como FTP, etc. se limita a aquellos que contengan información relacionada con la actividad del Consejo General de la Abogacía Española o con los cometidos del puesto de trabajo del usuario.
4. El Consejo General de la Abogacía Española se reserva el derecho de monitorizar y comprobar por ella misma o mediante la prestación de servicios de un tercero, de forma aleatoria y sin previo aviso, cualquier sesión de acceso a Internet iniciada por un usuario.
5. Cualquier fichero introducido en la red corporativa o en el terminal del usuario desde Internet deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.

D.5 Propiedad intelectual e industrial

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por la propiedad intelectual o industrial.

E. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS

1. Notificación

Cualquier persona que forme parte de la plantilla del Consejo General de la Abogacía Española o se halle prestando sus servicios temporalmente en la misma deberá notificar inmediatamente al responsable de seguridad cualquier anomalía que detecte y que afecte o pueda afectar a la seguridad de los datos.

El retraso en la notificación de incidencias constituirá un quebranto de la buena fe contractual, sancionable según las normas laborales de aplicación.

El procedimiento de notificación se realizará a través del correo electrónico y/o teléfono del responsable de seguridad.

2. Gestión

El responsable de seguridad recibirá las notificaciones de incidencias para proceder a su registro, y lo comunicará a los técnicos internos o externos encargados de la seguridad del sistema.

3. Respuesta

El responsable de seguridad se asegurará de que el departamento técnico da respuesta inmediata a la incidencia detectada y supervisará el trabajo de subsanación de la anomalía detectada. Una vez finalizada la subsanación, enviará un informe al responsable del fichero con todos los datos requeridos para el registro de la incidencia.

4. Registro

El responsable del fichero, de conformidad con el art. 10 del Real Decreto 994/1999, ha creado un registro en soporte electrónico en el cual se hace constar la siguiente información relativa a las incidencias:

- Tipo de incidencia
- Momento en el cual se ha producido la incidencia
- Persona que realiza la notificación
- Efectos derivados de dicha notificación.

Es obligación del responsable del fichero mantener actualizado el registro de incidencias.

Asimismo, es obligación del responsable de seguridad gestionar las incidencias que pudieran producirse, en el menor tiempo posible, garantizando, en la medida de lo posible, que la seguridad de los datos de carácter personal no se vea alterada en ningún momento.

En el registro de incidencias se consignarán, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Para la ejecución de los procedimientos de recuperación se precisará la autorización del responsable del fichero.

F. PROCEDIMIENTO DE REALIZACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS

F.1 Periodicidad de copias de respaldo

La realización de copias de seguridad de forma periódica permite al Consejo General de la Abogacía Española disponer de su información en caso de destrucción de los equipos o errores producidos en los datos y/o aplicaciones.

Existe una política de Backup determinada para cada entorno con una periodicidad de las copias de respaldo definida en función de la información que contengan. Estas políticas se encuentran documentadas.

F.2 Almacenamiento de las copias de seguridad

La realización de una doble copia de seguridad almacenando una de ella en los locales del CPD y otra en una ubicación externa minimiza el riesgo de pérdida de los datos en caso de producirse una contingencia.

Las copias de seguridad se guardan de forma segura en el centro de datos y en una caja de Seguridad en un Banco.

F.3 Protección de las copias de seguridad

La protección adecuada de las copias de seguridad permite, tanto su correcta conservación, como un control de acceso efectivo a los datos almacenados.

Las copias de respaldo se guardan en la zona de Seguridad del CPD en armarios bajo llave a los que sólo tiene acceso personal autorizado o en armarios ignífugos según criticidad. El acceso a la Caja de Seguridad del Banco está restringido también a personal autorizado.

F.4 Automatización del sistema de back-up

La automatización del procedimiento de back-up reduce la posibilidad de ciclos erróneos u omitidos.

F.5 Descripción de contenido de las copias de seguridad

La documentación del contenido de las copias de seguridad facilita su identificación.

En las etiquetas de las cintas está reflejado el contenido de esa copia. Esta misma información se guarda en una base de datos. Así mismo, se lleva un registro electrónico con los correos de verificación de la realización de la copia que recibe sistemas cuando ésta se ejecuta.

F.6 Control del almacenamiento

La existencia de un registro con el contenido de las copias de seguridad permite disponer de información sobre las copias de seguridad conservadas que faciliten un control efectivo en la gestión de la cintoteca.

El Departamento de Sistemas lleva un inventario manual del contenido de los backups ubicados en el banco actualizándose cada vez que se produce una entrada o una salida nueva. Las copias que permanecen en las oficinas están identificadas con etiquetas que permiten saber el contenido de las cintas.

F.7 Control de entrada y salida de las copias de seguridad

La existencia de un registro que controle las entradas y salidas de copias de seguridad provee de fiabilidad al inventario.

El inventario refleja todas las entradas y salidas de las copias de seguridad. En caso de que se solicite la retirada de alguna copia, quedará registrado también el solicitante de ésta y los motivos.

Para la retirada de información fuera de los locales del CPD con el fin de depositarlas en el centro de custodia externo se debe contar con una autorización expresa del Responsable de Seguridad. Se enviará la solicitud de retirada de dispositivos a la cuenta del responsable de seguridad indicando:

- Fecha de salida
- Motivo de la salida
- El tipo de soporte
- Código de soporte
- Tipo de información que contienen

El Responsable de Seguridad autorizará o rechazará la retirada.

F.8 Transporte de copias de seguridad

El transporte de las copias de seguridad debe contar con medios de seguridad adecuados que aseguren la no alteración, robo o destrucción de los datos en su fase de transporte.

F.9 Pruebas de restauración de copias de seguridad

La realización de pruebas de restauración de copias de seguridad confirma el funcionamiento correcto del proceso de recuperación de copias de datos y garantiza la integridad de los datos que estas contienen.

F.10 Período de existencia de copias de seguridad y su destrucción eventual

El establecimiento de un período de existencia de las copias de seguridad de acuerdo con la legislación vigente y la política de la sociedad, facilita la salvaguarda de las mismas y asegura el uso eficiente del espacio físico disponible para el almacenamiento.

El periodo de existencia de las copias de Seguridad vendrá definido en función de lo definido en su Política de Backup. Se estimará el tiempo estimado de vida de los dispositivos utilizados según su uso se procederá a la destrucción de los mismos cuando ésta llegue a su fin previa autorización por el Responsable de Seguridad

Anexo 2: ACRONIMOS

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónico CA (*Certification Authority*)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónico RA (*Registration Authority*)
ARL	*Authority Revocation List*, lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española
CPS	*Certification Practice Statement*, Declaración de Practicas de Certificación. también puede encontrarse identificada por el acrónico DPC
CRL	*Certifícate revocation list*, Lista de certificados revocados
CSR	*Certificate Signing request*, petición de firma de certificado
DES	*Data Encryption Estándar*. Estándar de cifrado de datos
DN	*Distinguished Name*, nombre distintivo dentro del certificado digital
DSA	*Digital Signature Algorithm*. Estándar de algoritmo de firma
DSCF	Dispositivo Seguro de Creación de Firma
FIPS	*Federal information Processing Estandar publication*
IETF	*Internet Engineering task force*
ICA	Ilustre Colegio de Abogados
ISO	*International Organisation for Standardization*. Organismo intenacional de estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones.
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso directorio
OCSP	*On-line Certificate Status Protocol*. Protocolo de acceso al estado del Certificado
OID	*Object identifier*. Identicador de Objeto
PA	*Policy Authority*. Autoridad de la Politica
PC	Política de Certificación puede encontrarse identificada por el acrónico CP (Certification Policy)
PIN	*Personal Identification Number*, Número de identificación personal
PKI	*Public Key Infrastructure*, Infraestructura de clave pública
PUK	*Personal Unblocking Key*, Código de desbloqueo
RSA	*Rivest-Shimar-Adleman*. Tipo de algoritmo de cifrado
SHA-1	*Secure Hash Algorithm*. Algoritmo seguro de Hash
SSL	*Secure Socket Layer*. Protocolo diseñado por Netscape y convertido en estándar en la Red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor
TCP/IP	*Transmission Control Protocol/Internet Protocol* Sistema de Protocolos, definidos en el marco de la IETFT. El Protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino, el Protocolo IP se encargará de direccional adecuadamente la información hacia su destinatario