Abogacía Española
CONSEJO GENERAL

AUTORIDAD DE CERTIFICACIÓN DE LA ABOGACÍA

Certificados cualificados de sello electrónico

Política de Certificación (CP7_ACA1_001.0)

Documento Público

CONTROL DE VERSIONES

Versión	Fecha	Descripción / Cambios Relevantes
001.0	18/07/2024	Primera versión

ÍNDICE

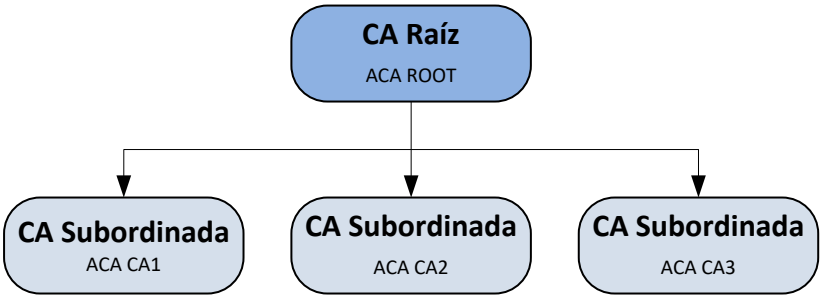
1. Introducción

1.1. Resumen

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.

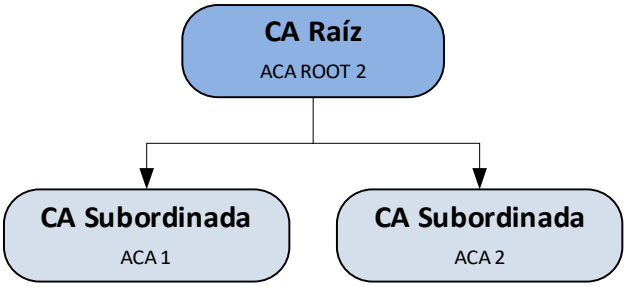
En el año 2016 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente.

Jerarquía 2016, compuesta de dos niveles:



En 2024 se han generado una nueva CA Raíz y CAs subordinadas en conformidad con la legislación vigente y se mantienen las descritas puesto que se encuentran en vigor los certificados expedidos por estas jerarquías teniendo una política de certificación propia. Los certificados definidos en esta política se expedirán mediante las nuevas CAs subordinadas.

Nueva Jerarquía 2024, compuesta de dos niveles;



El presente documento especifica la Política de Certificación del Certificado digital denominado "**Certificado Cualificado de Sello electrónico**" emitido por la autoridad de certificación del Consejo General de la Abogacía Española, o AC Abogacía.

El Consejo General de la Abogacía Española, como entidad reguladora de la abogacía, ha establecido un sistema propio 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 Política de Certificación está en conformidad con el REGLAMENTO (UE) No 910/2014, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE (de aquí en adelante Reglamento 910/2014), la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza (en adelante la Ley 6/2020) y las demás normas técnicas que regulan la identidad digital y los servicios de firma cualificada, cumpliendo todos los requisitos técnicos y de seguridad exigidos para emisión de Certificados Reconocidos y está basada en la especificación del estándar RCF 3647 – Internet X. 509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.

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

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

1.2. Identificación del documento

Nombre:	CP7_ACA1_001.0
O.I.D.	1.3.6.1.4.1.16533.50.7.1
Descripción:	Políticas de certificación (CP) de la Autoridad de Certificación de la Abogacía: Certificados cualificados de sello electrónico
Versión:	001.0
Fecha de Emisión:	18/07/2024
Localización:	www.acabogacia.org/doc
CPS relacionada	
O.I.D.	1.3.6.1.4.1.16533.10.1.1

Descripción:	Declaración de Prácticas de Certificación de la Autoridad de Certificación de la Abogacía
Localización:	www.acabogacia.org/doc

1.3. Comunidad y Ámbito de Aplicación.

1.3.1. Autoridad de Certificación (AC)

Es la entidad responsable de la emisión, y gestión de los certificados digitales. Actúa como tercera parte de confianza, entre el Suscriptor y el Usuario, en las relaciones electrónicas, esta Política permite identificar y vincular un determinado sistema o plataforma a una determinada entidad (Suscriptor) relacionada a un Colegio Profesional concreto a través de la emisión de un Certificado.

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

1.3.2. Autoridad de Registro (AR)

Ente que actúa conforme esta Política de Certificación y, en su caso, mediante acuerdo suscrito con la AC, cuyas funciones son la gestión de las solicitudes, identificación y registro de los solicitantes del Certificado y aquellas que se dispongan en las Prácticas de Certificación concretas.

A los efectos de la presente Política, la AR es el Consejo General de la Abogacía Española (CGAE)

1.3.3. Suscriptor

Bajo esta Política los suscriptores podrán ser los Colegios de profesionales, los Consejo General de las profesiones y los Consejos Autonómicos poseedor de un “Certificado Cualificado de Sello Electrónico” y, en general, cualquier persona jurídica vinculada o relacionada de alguna forma con las profesiones.

1.3.4. Usuario

En esta Política se entiende por Usuario, tercera parte confiante, la persona que voluntariamente confía en el Certificado, en virtud de la confianza depositada en la AC, lo utiliza como medio de identificación y autentificación de un sistema o aplicación así como medio para autenticar los documentos electrónicos que este produzca. y en consecuencia se sujeta a lo dispuesto en esta Política, en la Declaración de Prácticas de Certificación (CPS)aplicable y la legislación vigente, por lo que no se requerirá acuerdo posterior alguno.

1.3.5. Otros participantes

No estipulado

1.4. Ámbito de Aplicación y Usos

1.4.1. Usos permitidos de los certificados

El Certificado emitido bajo la presente Política permite identificar y vincular un determinado sistema o plataforma a una determinada entidad, ya sea un Colegio de profesional, un Consejo General de una

profesión o un Consejo Autonómico, así como cualquier persona jurídica vinculada al ejercicio profesional de la Abogacía, permitiendo además autenticar los documentos electrónicos que el Sistema produzca.

Los certificados cualificados emitidos bajo los criterios de esta política están indicados para soportar sello electrónico avanzado con certificados cualificados, garantizándose las condiciones establecidas en los artículos 36 y 37 eIDAS.

Los certificados de sello electrónico son certificados cualificados de acuerdo con lo que se establece en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y que dan cumplimiento a aquello dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones EN 319 412-5.

El uso del certificado de sello proporciona las siguientes garantías:

- No repudio de origen

  Asegura que el documento proviene de la entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica realizada por medio del sello electrónico. El receptor de un mensaje firmado electrónicamente podrá verificar el certificado empleado para esa firma utilizando cualquiera de los Prestadores de Servicios de Validación. De esta forma garantiza que el documento proviene de una determinada entidad, es decir la firma es la prueba efectiva del contenido y de la autoría del documento (garantía de “no repudio”).

- Integridad

  El certificado cualificado de Sello Electrónico, permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. Para garantizar la integridad, la criptografía ofrece soluciones basadas en funciones de características especiales, denominadas funciones resumen, que se utilizan siempre que se realiza una firma electrónica. El uso de este sistema permite comprobar que un mensaje firmado no ha sido alterado entre el envío y la recepción. Para ello se firma con la clave privada un resumen único del documento de forma que cualquier alteración del mensaje revierte en una alteración de dicho resumen.

1.4.2. Usos Prohibidos y no Autorizados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

Además, estos certificados serán utilizados por los firmantes en las relaciones que mantengan con terceros que confían, de acuerdo con los usos autorizados en las extensiones “Key Usage” y “Extended Key Usage” del certificado y en conformidad con las limitaciones que consten en el certificado.

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

1.5. Administración de la política

1.5.1. Organización responsable:

Autoridad de Certificación de la Abogacía.

Consejo General de la Abogacía Española

1.5.2. Persona de contacto

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

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

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

1.5.4. Procedimientos de aprobación de la Política

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

1.6. Definiciones y Acrónimos

AC	Autoridad de Certificación, también puede encontrarse identificada por el acrónico CA (*Certification Authority*)
ACA	Autoridad de Certificación de la Abogacía
AR	Autoridad de Registro también puede encontrarse identificada por el acrónico RA (*Registration Authority*)
ARL	*Authority Revocation List*, lista de certificados revocados de la Autoridad de Certificación Raíz
CGAE	Consejo General de la Abogacía Española

CPS	*Certification Practice Statement*, Declaración de Practicas de Certificación. también puede encontrarse identificada por el acrónico DPC
CRL	*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/ **DCCFE**	Dispositivo Seguro de Creación de Firma Dispositivo Cualificado de Creación de Firmas Electrónicas
eIDAS	Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
FIPS	*Federal information Processing Estandar publication*
IETF	*Internet Engineering task force*
ICA	Ilustre Colegio de Abogados
ISO	*International Organisation for Standardization*. Organismo intenacional de estandarización
ITU	*International Telecommunications Union.* Unión Internacional de Telecomunicaciones.
LDAP	*Lightweight Directory Access Protocol*. Protocolo de acceso directorio
OCSP	*On-line Certificate Status Protocol*. Protocolo de acceso al estado del Certificado
OID	*Object identifier*. Identicador de Objeto

PA	*Policy Authority*. Autoridad de la 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-2	*Secure Hash Algorithm*. Algoritmo seguro de Hash
TLS	*Transport Layer Security. Su antecessor es SSL (Secure Socket Layer es un p*rotocolo diseñado por Netscape y convertido en estándar en la Red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor)
TCP/IP	*Transmission Control Protocol/Internet Protocol* Sistema de Protocolos, definidos en el marco de la IETFT. El Protocolo TCP se usa para dividir en origen la información en paquetes, para luego recomponerla en destino, el Protocolo IP se encargará de direccional adecuadamente la información hacia su destinatario
ENS	Esquema Nacional de Seguridad. Adaptación de la norma ISO 27001 de la seguridad de la información al ámbito del Estado Español. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica
LOPDGDD	Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

2. Publicación y Repositorio de Certificados

2.1. Repositorios

AC Abogacía podrá a disposición de los usuarios la siguiente información

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

2.2. Repositorio de certificados

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

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

2.3. Frecuencia de publicación

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

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

Ordinariamente la AC publicará una lista de certificados revocados de oficio con una periodicidad de 24 horas. AC Abogacía publicará de forma extraordinaria una nueva lista de revocación en el momento en que tramita una petición de suspensión o revocación autenticada. No se realizan suspensiones.

2.4. Controles de acceso

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

En la web de AC Abogacía existirán accesos al directorio para la consulta de CRL y Certificados bajo el control de una aplicación y protegiendo la descarga indiscriminada de información. Las CRL's podrán descargarse de forma anónima mediante protocolo http desde la direcciones URL contenidas en los propios certificado en la extensión "CRL Distribution Point".

3. Identificación y Autenticación

3.1. Gestión de nombres

3.1.1. Tipos de nombres

Todos los certificados requieren un nombre distintivo (DN o distinguished name) conforme al estándar X.509, y los atributos especificados en la recomendación ITU-T X.520 [1]

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

- Un componente Nombre (Common Name) –CN
- Un componente E-mail –E
- Un componente Organización –O
- Un componente Identificador de la Organización –OI
- Un componente Unidad en la Organización –OU
- Un componente localidad- L
- Un componente Estado (Country) -C
- El valor autenticado del componente Nombre (Common Name) –CN contendrá la denominación del sistema o aplicación de proceso automático
- El valor autenticado del componente E-mail –E contendrá la dirección de correo de contacto de la entidad suscriptora del certificado
- El valor autenticado del componente Organización –O contendrá el nombre de la organización (suscriptor del certificado)
- El valor autenticado del componente Identificador de la Organización –OI contendrá una identificación del suscriptor diferente del nombre de la organización (suscriptor del certificado) en formato VATES – NIF entidad. Este valor cumplirá la semántica definida en el apartado 5, de ETSI EN 319 412-1 [i.4]
- El valor autenticado del componente Unidad en la Organización –OU contendrá la naturaleza del certificado (SELLO ELECTRONICO).
- El valor autenticado del componente Estado (Country)-C contendrá “ES”
- El valor autenticado del componente Localidad-L contendrá la ubicación de la sede social de la entidad suscriptora

3.1.2. Significado de los nombres

Los nombres incluidos en los certificados serán significativos y comprensibles.

3.1.3. Pseudónimos

Los certificados cualificados de sello electrónico no admiten pseudónimos.

3.1.4. Reglas utilizadas para interpretar varios formatos de nombres

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

3.1.5. Unicidad de los nombres

Los nombres distinguidos de los certificados emitidos serán únicos para cada suscriptor. La AC deberá realizar los esfuerzos que razonablemente estén a su alcance para confirmar la unicidad de los nombres de los certificados emitidos. El atributo de la Razón Social de la entidad, y/o el CIF darán para distinguir entre dos identidades cuando exista algún problema sobre duplicidad de nombres.

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

La AC no tiene responsabilidad en el caso de resolución de disputas de nombres. El Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza no deberá determinar que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado. Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

El Prestador de Servicios de Certificación / Prestador cualificado de servicios de confianza 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.

3.1.6. Reconocimiento, autenticación y función de las marcas registradas

No se admitirán marcas registradas como datos de identificación del Suscriptor. En todo caso se identificará a través de la Razón Social.

3.2. Validación inicial de la identidad

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

EL envío del PKCS10 por el suscriptor constituirá la garantía de que el suscriptor está en posesión de la clave privada.

3.2.2. Autenticación de la identidad de una organización

Se requerirá para todas las sociedades el Número de identificación fiscal (CIF) de la sociedad.

3.2.3. Autenticación de la identidad de un individuo

Para realizar una correcta verificación de la identidad del solicitante, se exigirá documentación que lo acredite y su personación física ante la AR y la presentación del Documento Nacional de Identidad o Tarjeta de Extranjero ante un operador o personal debidamente autorizado de la Autoridad de Registro y demostración de su vinculación con la persona jurídica.

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.

De acuerdo con el artículo 7 de la Ley 6/2020, Lo dispuesto en los párrafos anteriores podrá no ser exigible en los siguientes casos:

a) Cuando la identidad u otras circunstancias permanentes de los solicitantes de los certificados constaran ya a la AR en virtud de una relación preexistente, en la que, para la identificación del

interesado, se hubieran empleado los medios señalados en el párrafo primero y el período de tiempo transcurrido desde la identificación es menor de cinco años.

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

3.2.4. Comprobación de las facultades de representación

La AR verificará con sus propias fuentes de información el resto de datos y atributos a incluir en el certificado (subject), debiendo guardar la documentación acreditativa de la validez de aquellos datos no verificables por dichas fuentes.

3.2.5. Información de suscriptor no verificada

Toda la información contenida en los certificados será verificada.

3.2.6. Validación de las Autoridades de Registro

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS).

3.2.7. Criterios de interoperabilidad

No estipulado

3.3. Identificación y autenticación de renovación de certificados

3.3.1. Renovación ordinaria

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.

El proceso de renovación de un nuevo certificado, para el firmante es como si de una nueva emisión de certificados se tratase.

La renovación del certificado se podrá llevar a cabo de forma que se cumplan los requisitos que la Ley marca con respecto a los plazos máximos permitidos desde que la persona física realizó el registro presencial. En caso contrario, para renovar su certificado, tendrá que personarse en la oficina de registro siguiendo los procedimientos de comprobación de la identidad de persona física desarrollados a tal efecto.

3.3.2. Reemisión después de una revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

3.4. Identificación y autenticación de una solicitud de revocación

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

4. Requerimientos Operacionales del ciclo de vida del certificado

4.1. Solicitud de certificados

4.1.1. Quien puede solicitar un certificado

La AR gestiona las solicitudes de Certificados de sello electrónico

La solicitud de un certificado digital podrá realizarse personándose el solicitante en la Autoridad de registro ante un operador debidamente autorizado donde procederá a verificar y firmar el documento de conformidad con la emisión del certificado cualificado de Sello Electrónico de los datos de la solicitud, asumiendo la responsabilidad de la veracidad de la información reseñada y aportando además la documentación que acredite su representación y vinculación con la persona jurídica.

4.2. Tramitación de solicitud de certificados

Una vez recibida la solicitud del y antes de iniciar el proceso de emisión, la AR informa al solicitante del proceso de emisión, las responsabilidades y las condiciones de uso del certificado, así como verifica la identidad del solicitante, que la vinculación con la entidad para la que se solicita el sello electrónico es válida y tiene autorización para solicitarlo, por los medios de los que dispone el TSP y los datos a incluir en el certificado.

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

La firma del instrumento jurídico vinculante conlleva la aceptación los requisitos establecidos en la DPC y en esta PC.

El suscriptor debe generar el par de claves y un CSR que contiene una clave pública firmada electrónicamente mediante la clave privada asociada generada en dispositivo hardware o software, enviando por un canal seguro la clave pública junto con los datos verificados en formato PKCS10 u otro equivalente.

Tras la firma del instrumento jurídico vinculante, la Autoridad de Registro remitirá la solicitud a la Autoridad de Certificación de Abogacía de confianza para su tramitación.

Toda evidencia recogida durante el proceso, quedará vinculada al mismo y custodiada por la Autoridad de Certificación de la Abogacía.

4.3. Emisión de certificados

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

- La AR recibe la petición de emisión del certificado.
- La AR verificará la identidad del solicitante, su vinculación con la entidad a la que representa, autorización y los datos que se incluyan en el certificado dados de alta en el sistema.
- El solicitante enviará por un canal seguro un CSR en formato PKCS10 o equivalente, que previamente habrá generado en su sistema.

- El operador de la AR verifica nuevamente el contenido del mismo y si la verificación es correcta lo valida y tramita la aprobación de la emisión para la AC. Si la petición no es correcta, el operador deniega la petición.
- La AR envía por un canal seguro la petición a la AC para la emisión del correspondiente certificado.
- La AC emite el certificado el certificado x.509 de la clave pública asociada a su clave privada. El certificado generado es enviado de forma segura al solicitante.
- La AC notifica al suscriptor/solicitante la emisión del mismo.
- El certificado generado es enviado de forma segura al Registro de Certificados, que lo pone a disposición de los usuarios.

4.3.1. Actuaciones de la AC durante la emisión de los certificados

En la emisión de los certificados la AC:

• Utiliza un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada;

• Protege la confidencialidad e integridad de los datos de registro;

• Incluye en el certificado las informaciones establecidas en el artículo 6 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

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

En la finalización del proceso de emisión del Certificado cualificado, se informa al suscriptor que se encuentra disponible dicho certificado para su uso.

4.4. Aceptación de certificados

4.4.1. Forma en la que se acepta el certificado

A partir de la entrega del certificado, el suscriptor deberá revisar el mismo, determinar si es adecuado y si los datos se corresponden con la realidad. En caso de que existiera alguna diferencia entre los datos suministrados a la AC y el contenido del certificado, ello deberá ser comunicado de inmediato a la AC para que proceda a su revocación y a la emisión de un nuevo certificado.

La AC entregará el nuevo certificado sin coste para el suscriptor en el caso de que la diferencia entre los datos sea causada por un error no imputable al suscriptor.

La aceptación del certificado es la acción mediante la cual el suscriptor da inicio a sus obligaciones respecto a la Autoridad de Certificación de la Abogacía. El certificado se aceptará en el momento que el instrumento jurídico vinculante entre el firmante y ACA haya sido firmado y los medios que permitan hacer uso del certificado se encuentren en posesión del suscriptor.

Como evidencia de la aceptación deberá quedar una hoja de aceptación firmada por el firmante. El certificado se considera válido a partir de la fecha en que se firmó la hoja de aceptación.

4.4.2. Publicación del certificado por la AC

Los certificados no se publicarán en ningún repositorio de acceso libre.

4.4.3. Notificación de la emisión del certificado por la AC a otras Autoridades

No se efectúan notificaciones a terceros

4.5. Uso del par de claves y del certificado

4.5.1. Uso de las claves privada y el certificado por el suscritor

La clave privada será generada por el suscriptor y permanecerá en todo momento en posesión exclusiva del mismo.

Ni la AC ni ARs crean, almacenan ni poseen en ningún momento la clave privada del suscriptor, ni los datos de activación del dispositivo que la custodia.

El suscriptor sólo puede utilizar la clave privada y el certificado tras aceptar las condiciones de uso establecidas en la DPC y PC, el documento de aceptación medios y para los usos autorizados de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

El suscritor dejará de usar la clave privada tras la expiración o revocación del certificado.

Los certificados cualificados de Sello Electrónico regulados en esta PC permiten al titular aplicar de forma automatizada firma electrónica a documentos electrónicos.

4.5.2. Uso de la clave pública y certificado por un tercero que confía

Los terceros que confían en un certificado lo harán siempre de forma voluntaria asegurando que realizan las verificaciones oportunas que garantizan la validez del certificado en el que confían utilizando los medios sujetos siempre a las limitaciones que se establecen en la DPC y en esta PC y de acuerdo con lo establecido en las extensiones “Key Usage” y “Extended Key Usage” del certificado.

4.6. Renovación de certificados

Los certificados no podrán renovarse.

4.7. Renovación de certificados y claves

Ni los certificados ni las claves no podrán renovarse.

4.8. Modificación de certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

4.9. Suspensión y Revocación de certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

4.10. Servicios de comprobación del estado de los certificados

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

4.11. Finalización de la suscripción

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

4.12. Custodia y recuperación de claves

AC Abogacía no custodia ninguna clave privada de los usurarios por lo que no se podrán recuperar en ningún caso.

5. Controles de Seguridad Física, Procedimental y de Personal

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

6. Controles de Seguridad Técnica

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

Para las claves de la CA, según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

Las claves de los suscriptores son generadas por ellos mismos. La AC realizará los esfuerzos que razonablemente estén a su alcance para confirmar que las claves sean generadas de acuerdo a los estándares. El par de claves será generado y custodiado por el propio suscriptor o bajo su control.

Las claves de usuario son generadas usando el algoritmo de clave pública RSA, con los adecuados parámetros. Las claves tienen una longitud mínima de 3072 bits.

6.1.2. Entrega de la clave privada al suscriptor

No hay entrega por parte de la AC de claves privadas.

6.1.3. Entrega de la clave pública al emisor del certificado

La clave pública a ser certificada, es entregada a la Autoridad de Certificación mediante el envío de una solicitud de certificación en formato PKCS#10, de forma que se asegure que:

- No ha sido modificado durante el envío.
- El remitente está en posesión de la clave privada que corresponde con la clave pública transferida.
- El proveedor de la clave pública es el legítimo usuario que aparece en el certificado.

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

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.1.5. Tamaño de las claves

Las claves privadas del suscriptor están basadas en el algoritmo RSA con una longitud mínima de 3072 bits.

6.1.6. Parámetros de generación de la clave pública

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.1.7. Fines del uso de la clave

Todos los certificados incluirán la extensión Key Usage la cual se califica como crítica, indicando los usos habilitados de la clave.

Asimismo, pueden establecerse limitaciones adicionales mediante la extensión “Extended Key Usage”.

En el campo “key Usage” del certificado se ha incluido el siguiente uso:

Key Usage: nonRepudiation, DigitalSignature y Key Encipherment.

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

6.2.1. Estándares y controles de los módulos criptográficos

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

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

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.2.3. Custodia de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

La CA no custodia la clave privada de los certificados de sello. El usuario final es el encargado de su custodia, y éste será el responsable de mantenerla bajo su exclusivo control.

6.2.4. Backup de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

La AC no custodia ni hace backup la clave privada de los certificados de sello. El usuario final es el encargado de la custodia y en su caso del backup de la clave privada.

6.2.5. Archivo de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

Además, el usuario final también es el encargado de su archivado, y responsable de mantenerla bajo su exclusivo control.

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

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

La AC no custodia ni gestiona la clave privada de los certificados de sello.

6.2.7. Almacenamiento de la clave privada en módulo criptográfico.

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

Ni la AC ni la RA, almacenan ni poseen en ningún momento la clave privada del suscriptor, ni los datos de activación del dispositivo que la custodia.

6.2.8. Método de activación de la clave privada

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

6.2.9. Método de desactivación de la clave privada

La desactivación de la clave privada del suscriptor depende del dispositivo en el que esté generada. La desactivación se realizará cuando se cierre la aplicación software de creación de firma o el módulo criptográfico asociado.

6.2.10. Método de destrucción de la clave privada

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

Además, la destrucción de la clave privada del firmante consiste en borrar la clave privada y el certificado asociado al usuario del dispositivo software o hardware, según sea el caso. En cualquier caso será responsabilidad del suscriptor la correcta destrucción de la clave privada.

6.2.11. Evaluación del módulo criptográfico

No estipulado

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.3.2. Periodo de uso para las claves públicas y privadas

Determinado por el periodo de validez del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

La generación, custodia y gestión de la clave privada de los certificados de sello dependen exclusivamente del suscriptor.

6.4.2. Protección de datos de activación

Si las claves son generadas en software, se recomienda proteger los datos de activación de la clave privada, por medio de una contraseña. En el caso de emplear módulos criptográficos de seguridad, que se apliquen las medidas de seguridad que estos ofrecen activadas y un segundo factor cuando se emplea un QSCD.

6.4.3. Otros aspectos de los datos de activación

Sin especificar

6.5. Controles de seguridad informática

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.6. Requerimientos técnicos de seguridad informática específicos

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.7. Valoración de la seguridad informática

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.8. Controles de seguridad del ciclo de vida

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

6.9. Controles de seguridad de la red

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

6.10. Sellado de tiempo

No estipulado.

7. Perfiles de Certificado, CRL y OCSP

7.1. Perfil de Certificado

Todos los certificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3, la RFC 5280 "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*", ETSI EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile. y la RFC 3739 (que sustituye a RFC 3039) "*Qualified Certificates Profile*". También se ha tenido en cuenta la familia 319 412 en relación a los perfiles de los certificados.

Los certificados cualificados de sello electrónico incluirán, al menos, los siguientes datos:

una indicación, al menos en un formato adecuado para el procesamiento automático, de que el certificado ha sido expedido como certificado cualificado de sello electrónico;

un conjunto de datos que represente inequívocamente al prestador cualificado de servicios de confianza que expide los certificados cualificados, incluyendo como mínimo el Estado miembro en el que dicho prestador está establecido, y

a) para personas jurídicas: el nombre y, cuando proceda, el número de registro según consten en los registros oficiales,

b) para personas físicas, el nombre de la persona;

c) al menos, el nombre del creador del sello y, cuando proceda, el número de registro, tal como se recojan en los registros oficiales;

d) los datos de validación del sello electrónico que correspondan a los datos de creación del sello electrónico;

e) los datos relativos al inicio y final del período de validez del certificado;

f) el código de identidad del certificado, que debe ser único para el prestador cualificado de servicios de confianza;

g) la firma electrónica avanzada o el sello electrónico avanzado del prestador de servicios de confianza expedidor;

h) el lugar en que está disponible gratuitamente el certificado que respalda la firma electrónica avanzada o el sello electrónico avanzado a que se hace referencia en la letra g);

i) la localización de los servicios que pueden utilizarse para consultar el estado de validez del certificado cualificado;

j) cuando los datos de creación del sello electrónico relacionados con los datos de validación del sello electrónico se encuentren en un dispositivo cualificado de creación de sellos electrónicos, una indicación adecuada de esto, al menos en una forma apta para el procesamiento automático.

7.1.1. Número de versión

X509 Versión V3

7.1.2. Extensiones de certificado

7.1.2.1. Campos

Los certificados seguirán el estándar X509, definido en la RFC 5280, y tendrán los siguientes campos descritos en esta sección:

Certificados emitidos por ACA 1

CAMPOS	
Versión	V3
Nº Serie (Serial)	(nº de serie, que será un código único con respecto al nombre distinguido del emisor)
Algoritmo de Firma	ecdsaWithSHA256
Emisor (issuer)	CN = ACA CA1 O = CONSEJO GENERAL DE LA ABOGACIA ESPAÑOLA OI = VATES-Q2863006I OU = AUTORIDAD DE CERTIFICACION DE LA ABOGACIA C = ES
Valido desde (notBefore)	(fecha de inicio de validez, tiempo UTC)

Válido hasta (notAfter)	(fecha de fin de validez, tiempo UTC)
Asunto (Subject)	(Según especificaciones de la sección **3.1.1**)
Clave pública	RSA-3072 Bits o RSA-4096 Bits

7.1.2.2. Extensiones

Se incluirán las siguientes extensiones:

- Certificado cualificado de sello electrónico emitido por ACA 1

EXTENSIONES	VALOR
Identificador de clave del titular (SubjectKeyIdentifier)	Valor del identificador de clave del titular
Identificador de clave de entidad emisora (AuthorityKeyIdentifier)	Valor del Identificador de clave de entidad emisora
Uso mejorado de las claves (ExtendedKeyUsage)	Autenticación del cliente (1.3.6.1.5.5.7.3.2) Correo seguro (1.3.6.1.5.5.7.3.4)
Acceso a la Información de Autoridad (Authority Information Access)	[1]Acceso a información de autoridad Método de acceso=Protocolo de estado de certificado en línea (1.3.6.1.5.5.7.48.1) Nombre alternativo: Dirección URL=http://acaocsp.acabogacia.org/ [2]Acceso a información de autoridad Método de acceso=Emisor de la entidad emisora de certificados (1.3.6.1.5.5.7.48.2) Nombre alternativo: Dirección URL=http://acacert.acabogacia.org/aca1_cer.crt

Directivas de certificado (Certificate Policies)	[1] Directiva de certificados: Identificador de directiva= 1.3.6.1.4.1.16533.50.7.1 [1,1]Información de calificador de directiva: Id. de calificador de directiva=CPS Certificador: http://www.acabogacia.org/doc [2]Directiva de certificados: Identificador de directiva=0.4.0.194112.1.1 (qcp-legal)
Declaración de Certificados Calificados qcStatements x.509v3 certificate extension from RFC 3039	1.- id-etsi-qcs-QcCompliance 2.- QcEuRetentionPeriod: 15 años 4.- id-etsi-qcs-QcPDS URL=http://www.acabogacia.org/doc/EN 5.- QCSyntax-v2 id-etsi-qcs-SemanticsId-Legal: 0.4.0.194121.1.2 6.- QcType: id-etsi-qct-eseal: 0.4.0.1862.1.6.2
Punto de distribución de la CRL (CRLDistributionPoint)	http://acacrl.acabogacia.org/crl/aca1_crlN].crl https://acacrl.acabogacia.org/crl/aca1_crl[N].crl
Uso de la Clave (KeyUsage)	Firma digital, Sin repudio, Cifrado de clave

7.1.3. Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma será:

- 1.2.840.10045.4.3.2 ecdsaWithSHA256

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

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4. Formato de los nombres

Los certificados contienen el “distinguished name X.500” del emisor y del titular del certificado en los campos “issuer” y “subject” respectivamente.

7.1.5. Restricciones de nombre

No se emplean restricciones de nombres.

7.1.6. Identificador de objeto de política de certificado

Según el OID indicado en el apartado 1.2

7.1.7. Empleo de la extensión restricciones de política

No está definida

7.1.8. Sintaxis y semántica de los calificadores de política

La extensión "Certificate Policies" incluye.

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

Y el siguiente "Policy Identifier":

- QCP-l (0.4.0.194112.1.1): indicación de certificado cualificado de sello, acorde a eIDAS.

7.1.9. Tratamiento semántico para la extensión "Certificate policy"

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

7.2. Perfil de CRL

7.2.1. Número de versión

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

7.2.2. CRL y extensiones

- Para certificados emitidos con ACA 1

  http://acacrl.acabogacia.org/crl/aca1_crl[N].crl
  https://acacrl.acabogacia.org/crl/aca1_crl[N].crl

Se incluirán las siguientes extensiones

Extensiones
Versión
Emisor
Fecha Inicio de Validez
Fecha Fin de Validez

Algoritmo de Firma
Algoritmo Hash de firma
Identificador de la clave de autoridad
Número de CRL
CRL incluye certificados expirados

7.3. Perfil de OCSP

7.3.1. Número de versión

Los Certificados utilizados por el Servicio de información y consulta sobre el estado de validez de los certificados, vía OCSP, son conformes con el estándar X.509 versión 3.

7.3.2. Extensiones del OCSP

Las respuestas OCSP del Servicio de información y consulta sobre el estado de validez de los certificados son según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc.

8. Auditorias de conformidad

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

9. Otros temas legales y Operativos

Según lo dispuesto en la Declaración de Prácticas de Certificación (CPS). Consulte http://www.acabogacia.org/doc

ANEXO 1: Información técnica

En cumplimiento de lo establecido en el Reglamento 910/2014 y la Ley 6/2020, se informa a los suscriptores y usuarios de determinados aspectos en relación con dispositivos de creación y de verificación de firma electrónica que son compatibles con los datos de firma y con el certificado expedido, así como de mecanismos considerados seguros para la creación y verificación de firmas.

Los certificados cualificados emitidos bajo los criterios de esta política están indicados para soportar sello electrónico avanzado con certificados cualificados, tal y como está definido en el artículo 36 y 37 eIDAS, garantizando lo siguiente para todos los sellos:

a) estar vinculado al creador del sello de manera única;
b) permitir la identificación del creador del sello;
c) haber sido creado utilizando datos de creación del sello electrónico que el creador del sello puede utilizar para la creación de un sello electrónico, con un alto nivel de confianza, bajo su control exclusivo y
d) estar vinculado con los datos a que se refiere de modo tal que cualquier modificación ulterior de los mismos sea detectable.

Dispositivos del suscriptor

Creación y verificación de firmas

Estándares y parámetros admitidos

No estipulado.

Métodos de verificación de firmas

La comprobación de la firma electrónica es imprescindible para determinar que fue generada por el poseedor de claves, utilizando la clave privada correspondiente a la clave pública contenida en el certificado del suscriptor, y para garantizar que el mensaje o el documento firmado no fue modificado desde la generación de la firma electrónica.

La comprobación se ejecutará normalmente de forma automática por el dispositivo del usuario verificador, y en todo caso, y de acuerdo con la Declaración de Prácticas de Certificación (CPS)y la legislación vigente, con los siguientes requerimientos:

- Es necesario utilizar un dispositivo apropiado para la verificación de una firma digital con los algoritmos y longitudes de claves autorizadas en el certificado y/o ejecutar cualquier otra operación criptográfica.
- Es necesario establecer la cadena de certificados en que se basa la firma electrónica que debe verificarse y asegurarse que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica. Es responsabilidad y decisión del usuario que verifica la elección de la cadena apropiada si hubiera más de una posible.
- Es necesario comprobar la integridad, la firma digital y el estado de validez (no caducado, no revocado o no suspendido) de todos los certificados de la cadena con la información subministrada por AC Abogacía en su servicio de publicación de certificados. Sólo se puede considerar correctamente verificada una firma electrónica si todos o cada uno de los certificados de la cadena son correctos y vigentes.

- Es necesario verificar que los certificados de la cadena se han usado dentro de las condiciones y límites de uso que impone el emisor de cada uno de ellos, y por firmantes autorizados. Cada certificado de la cadena de certificación dispone de información sobre sus condiciones de uso y enlaces a documentación sobre los mismos.
- Es necesario verificar la adecuación de los algoritmos y parámetros de firma de todos los certificados de la cadena y del propio documento firmado.
- Es necesario determinar la fecha y hora de generación de la firma electrónica, ya que la verificación correcta exige que todos los certificados de la cadena fueran vigentes en el momento de generación de la firma.
- Es necesario, finalmente, determinar los datos firmados y verificar técnicamente la propia firma electrónica respecto del certificado utilizado para firmar, asociado a una cadena de certificación válida.

El usuario que verifica una firma debe actuar con la máxima diligencia antes de confiar en los certificados y las firmas digitales, y utilizar un dispositivo de verificación de firma electrónica con la capacidad técnica, operativa y de seguridad suficiente para ejecutar el proceso de verificación de firma correctamente.

Por último, los requisitos para la validación de sellos electrónicos cualificados vienen determinados en el artículo 40 del Reglamento 910/2014 (eIDAs).

El usuario que verifica será el responsable exclusivo del daño que pueda sufrir por la incorrecta elección del dispositivo de verificación, salvo que éste hubiere sido proporcionado por AC Abogacía.

El usuario que verifica tiene que tener en cuenta las limitaciones de uso del certificado indicadas de cualquier manera en el certificado, incluyendo aquellas no procesadas automáticamente por el dispositivo de verificación e incorporadas por referencia. Si las circunstancias requieren garantías adicionales, el verificador deberá obtener estas garantías para que la confianza sea razonable.

En cualquier caso, la decisión final respecto a confiar o no en una firma electrónica verificada es exclusivamente del usuario.

Verificación de la Firma Electrónica a lo largo del tiempo

- Si el usuario desea disponer de garantías a lo largo del tiempo que le permitan comprobar la validez de una firma electrónica, debe utilizar mecanismos adicionales, entre otros:
- Si el Firmante ha generado la firma en un formato capaz de verificarse a lo largo del tiempo, como los definidos en la norma EN 319 122-2 “Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 2: Extended CAdES signatures” del European Telecommunications Standards Institute (www.etsi.org), que AC Abogacía recomienda.
- Utilización por el firmante y el verificador de servicios de mediación de terceras partes, en los que ambos depositen su confianza, como:Servicios de validación de certificados o Servicios de sellado de tiempo o Servicios de notarización de transacciones o Etc
- Conservación, de manera segura e íntegra, junto con la firma de todos los datos necesarios para su verificación:
    - Todos los certificados de la cadena de certificación.
    - Todas las CRL vigentes inmediatamente antes y después del momento de la firma.
    - Las políticas y prácticas en vigor en el momento de la firma.