Política General de Certificación

Agencia Notarial de Certificación

ancert
Agencia Notarial de Certificación

Información general

Control documental

Proyecto:	Política general de certificación
Entidad de destino:	Agencia Notarial de Certificación, S.L.U.
Versión:	3.1
Fecha de la edición:	24/02/2022
Fecha de aprobación:	25/02/2022
Fecha de publicación:	05/04/2022
Archivo:	PG_Certificacion_ANCERT_20220405.docx
Formato:	Word 2019

Control de versiones

Versión	Partes que cambian	Descripción	Fecha cambio	Fecha publicación
2.0	Original	Creación del documento	27/03/2010	
2.1	Todo	Revisión del documento	05/05/2010	
2.2	Logo ANCERT	Cambio imagen corporativa	30/11/2010	
2.3	Todo	Revisión jurídica final antes de entrada en vigor	21/12/2010	01/01/2011
2.4	Sección 1.1.2	Añadidas las clases de certificados de cargo del CGN y certificados corporativos de servidor seguro. Corrección de erratas.	01/02/2011	01/03/2011
2.5	Secciones 4.9.6, 5.7.4 y 9.2	Adecuación controles AICPA/CICA WebTrust Program for CA v 2	01/06/2012	01/10/2012
2.6	Secciones 6.1 y 6.2	Adecuación de algunos puntos de los controles de protección de la clave privada a los requisitos AICPA/CICA WebTrust Program for CA v 2	29/09/2014	03/11/2014
2.7	Todo el documento	Adecuación de referencias y términos al Reglamento (UE) 910/2014.	04/05/2017	15/05/2017
2.8	Sección 9.4	Adecuación al Reglamente (UE) 2016/679 de tratamiento de datos personales.		25/05/2018
2.9	Secciones 3.3, 4.6 y 4.7 Sección 1.1.4 Sección 5.3.2 y 9.4	Carácter opcional de las renovaciones de los certificados. Se podrán renovar o no, en función de establecido en cada caso por la DPC correspondiente. Sello electrónico LOPDP 3/2018	01/04/2019	03/05/2019
3.0	Sección 1.5	Se establece la frecuencia de revisión y el proceso de aprobación del documento.	01/03/2020	06/04/2020

3.1	Sección 6.1	Actualización normas técnicas aplicables al QSCD y a los módulos HSM. Monitorización de la cualificación del QSCD y acciones a tomar en caso de la pérdida de la misma si hay certificados vigentes.	24/02/2022	05/04/2022

Índice

1. Introducción

Este documento contiene la política general de certificación de la Agencia Notarial de Certificación.

1.1. Presentación

1.1.1. Modelo de certificación

1. Esta sección describe el modelo de servicios de certificación de la Agencia Notarial de Certificación.

El modelo se construye a partir de tipos abstractos de certificados, mediante los cuales se especifican los perfiles concretos de certificados a producir.

Los certificados se definen por los siguientes criterios:

- Condición del destinatario del certificado.
    - Infraestructura.
    - Entidades finales.
- Comunidad a la que se dirige el servicio.
    - Propios.
    - Al público.
- Procedimientos de registro y entrega.
    - Colegiales.
    - Notariales.
    - Corporativos.
- Funcionalidad de uso de certificados de entidad final.
    - Firma electrónica.
    - Autenticación.
    - Cifrado.
    - Sistemas.
- Nivel legal de firma electrónica de las entidades finales.
    - Firma electrónica avanzada.
    - Firma electrónica cualificada.
- Firma electrónica a distancia:
    - Firma remota cualificada
    - Firma remota avanzada

- Persona identificada como firmante.
    - Persona física.
    - Persona jurídica.
    - Entidad sin personalidad.
- Persona identificada como suscriptor.
    - Individual.
    - Colectivo.
- Capacidad de actuación de la persona física.
    - Actuación en nombre propio.
    - Representación.

1.1.1.1. Certificados de infraestructura y de entidad final

En cuanto a la condición del destinatario del certificado, existen dos tipos de certificados:

1) Certificados de infraestructura, titularidad de la Agencia Notarial de Certificación, y que se emplean para producir certificados de autoridad de certificación, de fechado y otras funciones de infraestructura del servicio de certificación.
2) Certificados de entidad final, titularidad de los correspondientes suscriptores, que se emplean para usos finales, diferentes de la gestión de la infraestructura.

1.1.1.2. Certificados propios y al público

En cuanto a la comunidad a la que se dirige el servicio, existen dos tipos de certificados:

1) Certificados propios, expedidos a la comunidad cerrada de usuarios formada por Colegios de Notarios, Notarios y empleados/as de Notarías, y que no se expiden al público.
2) Certificados al público, expedidos en régimen de libre concurrencia en el mercado, a las entidades finales interesadas en los mismos.

1.1.1.3. Certificados colegiales, notariales y corporativos

En cuanto al procedimiento de registro y entrega, existen tres tipos de certificados:

1) Certificados colegiales. Son certificados expedidos por Colegios de Notarios a Notarios y a empleados de Colegios de Notarios y por Notarios a empleados de Notarías.
2) Certificados notariales. Son certificados expedidos por Notario a personas físicas, jurídicas o entidades sin personalidad jurídica.

3) Certificados corporativos[1]. Son certificados expedidos por corporaciones privadas a entidades finales.

1.1.1.4. Certificados de firma y certificados de sistemas

En cuanto a la funcionalidad de uso de los certificados de entidad final, existen dos tipos de certificados:

1) Certificados de firma electrónica, autenticación y cifrado. Son certificados empleados principalmente por personas para producir firmas, para autenticarse electrónicamente en sistemas informáticos y para cifrar documentos y mensajes.
2) Certificados de sistemas. Son certificados empleados principalmente por sistemas informáticos para usos diferentes de la producción de las firmas cualificadas.

1.1.1.5. Certificados de firma avanzada y de firma cualificada

En cuanto al nivel legal de firma electrónica producida por las entidades finales, existen dos tipos de certificados:

1) Certificados de firma electrónica avanzada. Son certificados cualificados, que funcionan en aplicaciones y programas de creación de firma electrónica.
2) Certificados de firma electrónica cualificada. Son certificados cualificados, que funcionan de forma conjunta con un dispositivo cualificado de creación de firma electrónica.

   Adicionalmente, ambos tipos de certificados se pueden emplear para firmar mensajes de autenticación (confirmación de la identidad), así como para firmar otros tipos de mensajes, y ofrecen funcionalidades de cifrado, pudiendo emplearse para producir o recibir documentos y mensajes cifrados, pero sin la posibilidad de recuperar la clave privada.

1.1.1.6. Firma electrónica a distancia

En cuanto a la generación de firmas electrónicas a distancia en un entorno de creación de firma electrónica gestionado por el prestador de confianza en nombre del firmante bajo el control exclusivo del firmante:

1) Certificado de firma electrónica remota cualificada. Son certificados cualificados que funcionan de forma conjunta con un dispositivo cualificado de creación de firma electrónica remota gestionado por el prestador de confianza.
2) Certificado de firma electrónica remota avanzada. Son certificados cualificados que funcionan de forma conjunta con un sistema de creación de firma electrónica remota gestionado por el prestador de confianza asegurando un control razonable del uso exclusivo de la clave del firmante.

[1] También se suelen denominar "certificados de redes privadas".

1.1.1.7. Certificados de persona física, de persona jurídica y de entidad sin personalidad jurídica

En cuanto a la persona identificada como firmante en el certificado, existen tres tipos de certificados:

1) Certificados de persona física, que actúa como firmante, en nombre propio o en representación de otra persona.
2) Certificados de persona jurídica, a la cual se imputan los documentos firmados, como firmante, en los casos expresamente previstos en la Ley, y sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.
3) Certificados de entidad sin personalidad jurídica, a la cual se imputan los documentos firmados, como firmante, en los casos expresamente previstos en la Ley, y sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.

1.1.1.8. Certificados individuales y de colectivo

En cuanto a la persona identificada como suscriptor en el certificado, existen dos tipos de certificados:

1) Certificados individuales, en que el suscriptor es la persona física.
2) Certificados de colectivo, en que el suscriptor es una persona jurídica o una entidad sin personalidad jurídica identificada en el certificado, mientras que la persona física actúa como poseedor de claves o firmante autorizado[2].

1.1.1.9. Certificados de actuación en nombre propio o de representación

En cuanto a la capacidad de actuación, existen dos tipos de certificados de persona física:

1) Certificados de actuación en nombre propio, de acuerdo con las reglas generales de capacidad de obrar.
2) Certificados de representación, en los que deben tomarse en cuenta los apoderamientos y capacidades de actuación de la persona, indicadas o no en el certificado, antes de confiar en la firma.

1.1.2. Matriz de clases y definiciones de certificados

Los anteriores criterios sirven, además, para la agrupación de las definiciones de certificados en clases o grupos de definiciones comunes de certificados.

[2] Por ejemplo, el certificado de un empleado de una empresa es de este tipo: mientras que la empresa es el suscriptor del certificado, el empleado es el poseedor de claves autorizado a firmar.

Las clases de certificados empleadas por la Agencia Notarial de Certificación para agrupar los servicios son las siguientes:

- **Clase Infraestructura**, que agrupa todos los certificados autoemitidos que sirven para ofrecer soporte a las operaciones de certificación. Estos certificados no se expiden al público en ningún caso.
- **Clase Consejo General del Notariado**, que agrupa todos los certificados de uso profesional por el colectivo de Notarios y sus empleados, incluyendo Colegios, cargos de la organización notarial y Notarías. Estos certificados no se expiden al público en ningún caso.
- **Clase Corporaciones de Derecho Público**, que agrupa todos los certificados al público, para uso profesional en el contexto de corporaciones de derecho público (distintas del Notariado).
- **Clase Notariales**, que agrupa todos los certificados expedidos al público con intervención notarial, aportando los máximos niveles de seguridad jurídica.
- **Clase Corporativos**, que agrupa todos los certificados expedidos al público con intervención de empresas actuando como entidades de registro diferentes de Notarios.

La Agencia Notarial de Certificación expedirá, al menos, los siguientes certificados:

- Clase Infraestructura.
    - Autoridad de Certificación.
    - Autoridad de Sellado de fecha y hora.
- Clase Consejo General del Notariado.
    - Notario/a (Certificado FEREN).
    - Certificados de Cargo.
    - Empleados/as.
- Clase Corporaciones de Derecho Público.
    - Personales de Corporaciones de Derecho Público.
    - De aplicación segura.
- Clase Notariales.
    - Personales.
        - Personales de representación personal.
    - Corporativos.
        - Corporativos de representación.
        - Facturación electrónica.
        - Sello electrónico.

  - Sistemas.
    - Servidor seguro.
    - Sellado de fecha y hora.
    - OCSP responder.
    - Firma de código.
    - Aplicación segura.
- Clase Corporativos.
  - Personales.
  - De aplicación segura.
  - Servidor seguro.

1.1.3. Definición de nuevos certificados

La definición de nuevos certificados y su incorporación dentro de la matriz anteriormente indicada deberá ser realizada mediante el siguiente procedimiento:

- Debe describirse el certificado como una combinación concreta de las características y condiciones establecidas en la sección 1.1.1 de esta política.
- Cuando la definición obtenida resulte diferente de las definiciones de certificados previamente existentes, se nombrará la definición y se incorporará a la matriz, dentro de una de las clases existentes.
- Cuando exista un certificado ya definido con una definición equivalente a la descripción del nuevo certificado, en lugar de incorporar el nuevo certificado a la matriz se ampliará la definición del certificado previamente existente.
- Cuando exista un certificado ya definido con una definición similar a la descripción del nuevo certificado, el nuevo certificado se tratará como un subtipo del certificado previamente existente.

1.1.4. Los servicios de validación e información

La Agencia Notarial de Certificación podrá prestar servicios de validación e información en relación con los certificados, tanto expedidos de acuerdo con esta política como por otros prestadores de servicios de certificación.

1.2. Nombre del documento e identificación

Este documento es la "Política general de certificación de la Agencia Notarial de Certificación".

La Agencia Notarial de Certificación debe asignar a cada tipo de certificado un identificador de objeto (OID), para su identificación por las aplicaciones, que constará en la correspondiente Declaración de Prácticas de Certificación.

Adicionalmente, la Agencia Notarial de Certificación publicará en su Depósito un documento con los OIDs correspondientes a las políticas de certificación vigentes en cada momento.

1.3. Participantes en los servicios de certificación

Esta política de certificación regula la prestación de servicios de certificación a comunidades cerradas de usuarios y al público. Los certificados expedidos a las comunidades cerradas de usuarios no se expiden al público.

Las comunidades cerradas de usuarios podrán ser:

- El Notariado español, comunidad a la que se emiten certificados para diversos usos y aplicaciones profesionales relacionadas con las entidades que lo integran.
- Las Corporaciones de Derecho Público, comunidad a la que se emiten certificados para sus propios usos.

En segundo lugar, esta política regula la prestación por la Agencia Notarial de Certificación, de servicios de certificación al público, principalmente con la colaboración de los Notarios, así como de otras entidades privadas.

Los participantes en los servicios de certificación serán los siguientes.

1.3.1. Prestador de Servicios de Certificación

La Agencia Notarial de Certificación actuará como única prestadora de servicios de certificación, por encargo del Consejo General del Notariado de España.

La Agencia Notarial de Certificación podrá disponer de una o más Entidades de Certificación para la prestación de los servicios, de acuerdo con los siguientes criterios:

- Pueden crearse diversas Entidades Raíz de Certificación, agrupando las políticas de certificados por clases. En cualquier caso, debería existir al menos una única Entidad Raíz para cada una de las clases de certificados, con excepción de la clase de infraestructura.
- Dependiendo de las anteriores entidades, pueden crearse diversas Entidades Subordinadas de Certificación, pudiendo existir únicamente una Entidad de Certificación para cada política de certificación y sus subtipos.

1.3.2. Entidades de registro

Las entidades de registro serán las personas físicas o jurídicas que asisten a la Agencia Notarial de Certificación en las tareas de emisión y gestión de los certificados, y en concreto, en las tareas de:

- Contratación del servicio de certificación a entidades finales.

- Identificación y autenticación de la identidad y circunstancias personales de las personas que reciben los certificados.
- Generación de certificados y entrega de dispositivos seguros de creación de firma a los suscriptores.
- Almacenamiento de documentos en relación con los servicios de certificación.

1.3.3. Entidades finales

Las entidades finales serán las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para firma, autenticación y cifrado, y entre ellas, las siguientes:

1) Solicitantes de certificados, que los solicitan para ellos o para terceras personas.
2) Suscriptores de certificados, que ostentan la titularidad de los certificados.
3) Poseedores de claves, que las emplean para las finalidades y aplicaciones previstas en los certificados.
4) Representados.
5) Terceros que confían en certificados.

1.3.3.1. Solicitantes de certificados

Todo certificado debe ser solicitado por una persona, en su propio nombre (certificados de persona física) o en nombre de una organización (certificados de persona jurídica o entidad sin personalidad jurídica).

Pueden ser solicitantes de certificados:

1) La persona que va a ser el futuro suscriptor del certificado (certificados individuales o de persona física), y, en consecuencia, el poseedor de claves.
2) La persona que, sin ser el futuro suscriptor del certificado solicitado, va ser el poseedor de claves (obligatoriamente en el caso de certificados de persona jurídica o de entidad sin personalidad jurídica, y opcionalmente en el caso de los restantes certificados de colectivo).
3) La persona que, sin ser el futuro suscriptor ni el futuro poseedor de claves del certificado, solicita el certificado para otra persona física, en los casos de delegación de facultades del solicitante.

1.3.3.2. Suscriptores de certificados

Los suscriptores son las personas y las organizaciones titulares del certificado.

En certificados individuales, el suscriptor coincide con el poseedor de claves. En certificados de colectivo, el suscriptor es una entidad y el poseedor de claves, una persona física autorizada o apoderada para recibir y emplear el certificado.

La capacidad del poseedor de claves para actuar en nombre y representación del suscriptor de certificados de colectivo deberá establecerse en el propio certificado, de acuerdo con los requisitos de esta política.

1.3.3.3. Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves criptográficas. El poseedor de claves coincide con el concepto de firmante empleado en la legislación de firma electrónica, pero se denomina de esta forma genérica, dado que también puede emplear el certificado para otras funciones, como la autenticación o el descifrado.

Los poseedores de claves se encuentran debidamente identificados en el certificado, mediante su nombre apellidos, o, en determinados casos, mediante el empleo de seudónimos.

La capacidad del poseedor de claves para actuar en nombre y representación del suscriptor de certificados de colectivo deberá establecerse en el propio certificado, de acuerdo con los requisitos de esta política.

1.3.3.4. Representados

Tendrán la consideración de representados las personas físicas o jurídicas en cuyo nombre los solicitantes solicitan certificados de representación, de persona jurídica o de entidad sin personalidad jurídica, sin perjuicio de su posible condición de suscriptor, en caso de certificados de colectivo.

1.3.3.5. Terceros que confían en certificados

Los terceros que confían en certificados son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, los terceros deben verificarlos, tal como se establece en este documento de política y en los documentos jurídicos correspondientes.

1.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, de acuerdo con la tipología indicada en la sección 1.1.1 de esta política general, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

La Declaración de Prácticas de Certificación correspondiente determinará los usos concretos de cada certificado emitido, de acuerdo con las normas establecidas en esta sección.

1.4.1. Usos permitidos para los certificados

1.4.1.1. Certificados de infraestructura y de entidad final

Los certificados de infraestructura se emplean exclusivamente por la Agencia Notarial de Certificación para la prestación de servicios de certificación y otros servicios relacionados.

Los certificados de entidad final se emplean para los diversos usos definidos en cada Declaración de Prácticas de Certificación, con exclusión de la posibilidad de funcionar como certificados de infraestructura.

1.4.1.2. Certificados de firma electrónica y certificados de sistemas

Los certificados de firma electrónica se emplean para la autenticación, firma y, en su caso, protección criptográfica de actos documentados electrónicamente por personas.

Los certificados de sistemas, por su parte, se emplean para finalidades distintas de la firma personal, como la protección de redes de comunicaciones electrónicas, así como de los servidores y agentes que interactúan en las citadas redes, o para la protección del código que circula a través de las mismas.

1.4.1.3. Certificados de firma electrónica avanzada y de firma electrónica cualificada

Los certificados de firma electrónica - y otros usos - son certificados cualificados, de acuerdo con lo establecido en el Reglamento (UE) 910/2014, con el contenido prescrito por el Anexo I del mismo Reglamento, de acuerdo con lo establecido en la especificación técnica EN 319 411-2 v2.1.1, del Instituto Europeo de Normas de Telecomunicaciones.

Los certificados de firma electrónica cualificada funcionan de forma conjunta con un dispositivo cualificados de creación de firma electrónica, que cumple los requisitos establecidos por el artículo 29 del Reglamento (UE) 910/2014 y esta política; mientras que los certificados de firma electrónica avanzada no ofrecen esta garantía.

Los certificados de firma electrónica cualificada pueden emplearse, en general, para la realización de cualquier acto jurídico documentado electrónicamente, en especial cuando la realización del mismo documento en soporte papel exija la firma manuscrita, y siempre que el certificado no incorpore límites que lo impidan.

Por su parte, los certificados de firma electrónica avanzada pueden emplearse conforme a las condiciones acordadas por las partes para relacionarse entre sí, o cuando la normativa administrativa aplicable lo admita expresamente.

Asimismo, los certificados permiten otras funcionalidades adicionales, como la autenticación o el cifrado y descifrado de mensajes y documentos por parte del suscriptor o del poseedor de claves.

1.4.1.4. Certificado de sello electrónico

Los certificados de sello electrónico son certificados cualificados de sello electrónico de acuerdo con los establecido en el Reglamento (UE) 910/2014, con el contenido prescrito por el Anexo III del mismo reglamento, de acuerdo con lo establecido en la especificación técnica EN 319 411-2 v2.1.1, del Instituto Europeo de Normas de Telecomunicaciones.

Los certificados cualificados de sello electrónico vinculan los datos de validación de un sello con una persona jurídica y confirma el nombre de la persona.

Los certificados cualificados de sello electrónico empleados de forma conjunta con un dispositivo cualificado de creación de sello electrónico, que cumple *mutatis muntandis* los requisitos establecidos por el Anexo II del Reglamento (UE) 910/2014, permiten la generación de sellos electrónicos cualificados; mientras que los certificados de sello cualificados sin dispositivo cualificado no ofrecen esta garantía.

Los certificados de sello electrónico cualificado pueden emplearse, en general, para la generación de sellos electrónicos.

Asimismo, los certificados permiten otras funcionalidades adicionales, como la autenticación o el cifrado y descifrado de mensajes y documentos por parte del suscriptor o del poseedor de claves.

1.4.1.5. Certificados de persona física, de persona jurídica y de entidad sin personalidad jurídica

Los certificados de persona física deben ser empleados para actos realizados por la persona física suscriptora de los mismos, en su propio nombre o en representación de un tercero, con sujeción a los requisitos generales de capacidad de obrar personal, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido.

Los certificados de persona jurídica deben ser empleados de acuerdo con lo establecido en el artículo 7 de la Ley 59/2003, de 19 de diciembre, de firma electrónica, en el ámbito de las Administraciones Públicas y en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario, entendiendo por tal, las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de la actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido.

Con la entrada en vigor del Reglamento (UE) 910/2014 el 1 de Julio de 2016, a partir de esa fecha, no se emitirán nuevos certificados para personas jurídicas.

Los certificados de entidad sin personalidad jurídica propia deben ser empleados exclusivamente en el ámbito tributario, de acuerdo con lo establecido en la disposición adicional tercera.

1.4.1.6. Certificados individuales y de colectivo

Los certificados de colectivo deben ser empleados siempre de acuerdo con las instrucciones del colectivo suscriptor de los mismos.

1.4.1.7. Certificados de actuación en nombre propio o de representación

Los certificados de actuación en nombre propio deben ser empleados exclusivamente para la realización de actos personales, con sujeción a los requisitos generales de capacidad de obrar personal.

Los certificados de representación deben ser empleados únicamente dentro de las facultades de representación otorgadas o delegadas.

1.4.2. Límites y prohibiciones de uso de los certificados

1.4.2.1. Límites de uso

Los certificados se emplearán para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

Los certificados pueden incorporar límites de uso por razón de la cuantía y de la materia, que se establecen en una extensión del certificado registrada por la Agencia Notarial de Certificación.

En el caso de certificados de representación, dichos límites deben resultar consecuentes, en su caso, con el documento público, administrativo o judicial en el que se base la representación.

Del mismo modo, los certificados deberán emplearse únicamente de acuerdo con la ley aplicable, especialmente teniendo en cuenta las restricciones de importación y exportación existentes en cada momento.

Aunque los certificados de entidad final se pueden emplear, con algunas excepciones, para el cifrado o descifrado de documentos electrónico, se advierte que dichos usos se realizan bajo la exclusiva responsabilidad del suscriptor o del poseedor de claves, según proceda.

1.4.2.2. Prohibiciones de usos

Los certificados de entidad final no pueden emplearse para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (CRL) o informaciones de estado de certificados (mediante servidores OCSP o similares), excepto cuando se autorice expresamente.

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.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de usos limitados y/o prohibidos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor, el poseedor de claves o los terceros perjudicados reclamar a la Agencia Notarial de Certificación, o al Consejo General del Notariado, compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para los usos limitados y/o prohibidos.

1.5. Administración de la política

1.5.1. Organización que administra el documento

Agencia Notarial de Certificación S.L.U.

1.5.2. Datos de contacto de la organización

Agencia Notarial de Certificación S.L.U.

Paseo del General Martínez Campos 46, 6ª planta

28010 Madrid

Teléfono: 912187676

ancert@ancert.com

1.5.3. Responsable de adecuación de la Declaración de Prácticas de Certificación

Quien determina la conformidad de la Política General y las Declaraciones de Prácticas es el responsable del Servicio de Certificación de la Agencia Notarial de Certificación.

1.5.4. Procedimiento de aprobación de la Declaración de Prácticas de Certificación

Existe un procedimiento de creación, revisión y aprobación formal que garantiza el correcto mantenimiento de este documento. El Comité de Seguridad de la Agencia Notarial de Certificación es el órgano responsable de la aprobación.

1.5.5. Frecuencia de revisión

La Política General de Certificación, las Declaraciones de Prácticas y los textos divulgativos son revisados y, si procede, actualizados, con una periodicidad anual.

2. Publicación de información y depósito de certificados

2.1. Depósito(s) de certificados

La Agencia Notarial de Certificación deberá disponer de un Depósito de certificados.

El servicio de Depósito estará disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control del prestador de servicios de certificación, éste realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 y la Declaración de Prácticas de Certificación aplicable.

2.2. Publicación de información del prestador de servicios de certificación

La Agencia Notarial Certificación publicará las siguientes informaciones, en su Depósito:

- Los certificados emitidos, incluidos de los certificados de Entidades de Certificación.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.

- La política general de certificación del Consejo General del Notariado, así como cualesquiera políticas específicas de certificados dictadas por la Agencia Notarial de Certificación para desarrollar ulteriores requisitos, dentro del marco de esta política.
- Las Declaraciones de Prácticas de Certificación.
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en certificados.

El Depósito debe contener las versiones vigentes en cada momento, así como el histórico de versiones anteriores.

2.3. Frecuencia de publicación

La información anteriormente indicada, incluyendo políticas y la Declaración de Prácticas de Certificación, se publicará en cuanto se encuentre disponible.

Los cambios en los documentos de política y en la Declaración de Prácticas de Certificación se regirán por lo establecido en la sección 1.5 del documento de política o Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publicará de acuerdo con lo establecido en las secciones 4.9.6 y 4.9.7 de esta política.

2.4. Control de acceso

La Agencia Notarial de Certificación no limitará el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establecerá controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información de estado de revocación.

El prestador de servicios de certificación empleará sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si el suscriptor ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3. Identificación y autenticación

3.1. Gestión de nombres

3.1.1. Tipos de nombres

Todos los certificados contendrán un nombre diferenciado de la persona y/o organización, identificados en el certificado, definido, siempre que resulte compatible, de acuerdo con lo

previsto en la Recomendación ITU-T X.501 y contenido en el campo *Subject*, incluyendo un componente *Common Name*.

Los certificados podrán contener nombres alternativos de las personas y organizaciones identificadas en los certificados, principalmente en el campo *SubjectAlternativeName*, como el correo electrónico.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados deberán incluirse en atributos predefinidos en normas y especificaciones técnicas ampliamente utilizadas en el sector o sectores de actividad donde deban emplearse los certificados.

En caso de que determinadas circunstancias personales no sean fácilmente representables mediante las normas y especificaciones técnicas anteriormente reseñadas, la Agencia Notarial de Certificación deberá establecer extensiones privadas de certificados y atributos privados para incluir dichas informaciones en los certificados.

3.1.2. Significado de los nombres

Los nombres de los certificados serán comprensibles e interpretados de acuerdo con la legislación aplicable a los nombres de las personas físicas y jurídicas titulares de los certificados, según se indica en el componente *Country* del nombre.

Los nombres incluidos en los certificados serán tratados de acuerdo con las siguientes normas:

- Se codificará el nombre tal y como aparece en la documentación acreditativa.
- Se podrán eliminar los acentos, para garantizar la mayor compatibilidad técnica posible.
- Los nombres podrán ser adaptados y reducidos, al objeto de garantizar el cumplimiento de los límites de longitud aplicables a cada campo del certificado.

3.1.3. Empleo de anónimos y seudónimos

En ningún caso se pueden emitir certificados anónimos.

Cuando ninguno de los usos potenciales sea la relación electrónica con las Administraciones Públicas, podrá existir un tipo de certificado, o una política especial de certificación que admita el empleo de seudónimos.

En ningún caso podrán emitirse, bajo una misma política, certificados con seudónimos y certificados indicando la identidad real, debiendo hacerse mediante políticas diferentes o mediante una política específica de una política existente.

3.1.4. Interpretación de formatos de nombres

La Agencia Notarial de Certificación podrá emplear, en general, el esquema de nombres que considere más apropiado, de acuerdo con las siguientes normas:

- Cuando alguno de los usos potenciales, de los autorizados por el certificado, sea establecer relaciones electrónicas con las Administraciones Públicas, debe ser un formato de nombres

admisible por las Administraciones Públicas y, en particular, compatible con las restricciones establecidas por la AEAT.

- Todos los certificados de firma incluirán la siguientes informaciones obligatoriamente:
    - Una mención al país, contenida en el componente *Country*, que se empleará para identificar la nacionalidad del suscriptor o del poseedor de claves, según proceda.
    - El nombre y apellidos de la persona física identificada en el certificado, y su número de documento nacional de identidad o equivalente, debiendo contenerse en una combinación de los siguientes componentes: *Common Name, Given Name, Surname, Serial Number* y, cuando el certificado deba ser admitido en las relaciones con la AEAT, el componente específico definido por la AEAT para el número de documento nacional de identidad o equivalente del custodio de los certificados de persona jurídica y entidad sin personalidad jurídica.
- Los certificados de la clase Consejo General del Notariado deberán incluir las siguientes informaciones adicionales:
    - Una indicación a la población correspondiente a la notaría o Colegio Notarial, contenida en el componente *Locality Name*.
    - Una indicación a la provincia correspondiente a la notaría o Colegio Notarial, contenida en el componente *State or Province Name*.
    - Una mención al Colegio Notarial, contenida en un componente *Organizational Unit Name*.
    - Una mención al código de notaría o al código del cargo, en su caso, contenida en un componente *Organizational Unit Name*.
- Los certificados de la clase Corporaciones de Derecho Público deben incluir las siguientes informaciones adicionales:
    - Una mención a la corporación, contenida en el componente *Organization*
- Los certificados de la clase Notariales deberán incluir las siguientes informaciones adicionales:
    - Una mención al tipo de certificado, contenida en el componente *Organizational Unit Name*.
    - Una mención al notario/a autorizante, contenida en un componente *Organizational Unit Name*
    - Cuando indiquen la representación, una mención al nombre y apellidos, y número de identificación fiscal del representado, o la razón social y código de identificación fiscal del representado, según proceda.
    - Los certificados de sistemas tendrán sus propias normas, adaptadas a las necesidades concretas de cada tipo de certificado, debiendo indicar en todo caso la

persona o entidad titular y las informaciones técnicas apropiadas, como el dominio o la aplicación.

La Agencia Notarial de Certificación deberá publicar en el Depósito la información sobre la sintaxis y la semántica necesaria para el tratamiento de dichas extensiones y atributos privados, por parte de los terceros.

3.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos para cada Entidad de Certificación operada por la Agencia Notarial de Certificación. Una persona sólo podrá tener más de un certificado con el mismo nombre a la vez, durante el período de renovación de certificados, para garantizar la continuidad de sus operaciones.

En ningún caso se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente.

3.1.6. Resolución de conflictos relativos a nombres

En los certificados de clase Consejo General del Notariado y clase Corporaciones de Derecho Público, además del número del Documento Nacional de Identidad o equivalente, se podrá incluir el número de colegiado o de personal administrativo, cuando éstos existan.

En los restantes certificados de firma, los conflictos de nombres de poseedores de claves que aparezcan identificados en los certificados con su nombre real se solucionan mediante la inclusión, en el nombre diferenciado del certificado, del número del Documento Nacional de Identidad, o equivalente, del poseedor de la clave, así como del número del Código de Identificación Fiscal de la persona jurídica, según proceda.

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

La Agencia Notarial de Certificación no estará obligada a determinar previamente que un solicitante de certificados tiene derecho sobre una marca o dominio incluidos en una solicitud de certificado, sino que en principio procederá a certificarlo.

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.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación española, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, la Agencia Notarial de Certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

3.2. Validación inicial de la identidad

En esta sección se establecen requisitos relativos a los procedimientos de identificación y autenticación que deben emplearse durante el registro de suscriptores, incluyendo colectivos y personas físicas, que debe realizarse con anterioridad a la emisión y entrega de certificados.

3.2.1. Prueba de posesión de clave privada

Esta sección describe los métodos a emplear para demostrar que se posee la clave privada correspondiente a la clave pública objeto de certificación.

El método de demostración de posesión de la clave privada será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método fiable aprobado por la Agencia Notarial de Certificación.

Este requisito no se aplica cuando el par de claves es generado por la entidad de registro, por delegación del suscriptor, durante el proceso de personalización o de entrega del dispositivo cualificado de creación de firma al suscriptor o poseedor de claves.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del dispositivo cualificado y del correspondiente certificado y par de claves almacenados en su interior.

3.2.2. Autenticación de la identidad de una organización

Esta sección contiene requisitos para la comprobación de la identidad de una organización identificada en el certificado o que interviene en procesos de certificación digital.

La Agencia Notarial de Certificación debe autenticar, con carácter previo a la emisión y entrega de un certificado de colectivo, la identidad del suscriptor y otros datos, de acuerdo con lo establecido en la sección 3.1.

El prestador de servicios de certificación podrá emplear entidades de registro para esta tarea, pudiendo emplear los siguientes métodos:

1) Obtención de información acerca de la organización, de un proveedor externo de servicios de esta naturaleza, a discreción de la Agencia Notarial de Certificación, que previamente deberá aprobar al proveedor externo.
2) Comprobación de documentación justificativa aportada por el solicitante, acerca de los siguientes extremos:
    - Nombre legal completo de la organización.
    - Estado legal de la organización.
    - Número de identificación fiscal.
    - Datos de identificación registral.

Las declaraciones de prácticas de certificación determinarán los métodos a emplear y el procedimientos de autenticación apropiado para cada caso.

No será necesario autenticar la identidad de los Colegios profesionales y otras organizaciones que actúan como entidades de registro, dado que dicha identidad ya ha sido debidamente autenticada previamente en el establecimiento de la relación jurídica con la Agencia Notarial de Certificación.

3.2.3. Autenticación de la identidad de una persona física

Esta sección contiene requisitos para la comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1. Elementos de identificación requeridos

La Agencia Notarial de Certificación establecerá el número y los tipos de documentos que sean necesarios para acreditar la identidad del poseedor de la clave, pudiendo emplear los siguientes:

1) Documento Nacional de Identidad.
2) Tarjeta de Identificación de Extranjero.
3) Pasaporte.

Dichos documentos deberán contener las siguientes informaciones:

1) Nombre y apellidos.
2) Fecha de nacimiento.
3) Número de identidad reconocido legalmente.
4) Otros atributos necesarios, de acuerdo con la política aplicable.

3.2.3.2. Validación de los elementos de identificación

La información de identificación de suscriptores de certificados individuales, así como de poseedores de claves de certificados de colectivo, se realiza contrastando la información de la solicitud con la documentación aportada, electrónicamente o en soporte físico, por parte de la entidad de registro correspondiente.

3.2.3.3. Necesidad de presencia personal

En general, se requiere presencia física directa del solicitante de certificados y, en su caso, de la persona física a identificar en el mismo, para la obtención de certificados.

En el caso de los certificados de la clase Corporaciones de Derecho Público y clase Corporativos, se pueden emplear métodos basados en la presencia física indirecta, cuando la validación de la identidad se ha producido en forma personal anteriormente y los registros corporativos se mantienen permanentemente actualizados.

Se deberá garantizar, en cualquier caso, la entrega y aceptación del certificado por el suscriptor o poseedor de claves, según proceda.

3.2.3.4. Vinculación de la persona física con una organización

En los certificados de colectivo y en los certificados de representación se debe identificar y autenticar la vinculación de la persona física con la organización, mediante procedimientos adecuados a cada política de certificación.

3.2.4. Información de suscriptor no verificada

No se podrá incluir información de suscriptor no verificada en los certificados.

3.3. Identificación y autenticación de solicitudes de renovación

3.3.1. Validación para la renovación rutinaria de certificados

Se podrán renovar certificados, durante su periodo de vigencia (de acuerdo a lo establecido en la DPC correspondiente).

Antes de renovar un certificado, la Agencia Notarial de Certificación o las entidades de registro correspondientes deberán comprobar que la información empleada para verificar la identidad y los restantes datos del suscriptor y del poseedor de la clave continúan siendo válidos.

Se podrá emplear la firma electrónica basada en un certificado para solicitar la renovación del mismo, siempre antes de su expiración. Posteriormente podrán emplearse otros mecanismos, siempre que resulten suficientemente fiables.

Si cualquier información del suscriptor o del poseedor de la clave hubiere cambiado, se registrará adecuadamente la nueva información, de acuerdo con lo establecido en la sección 3.2.

3.3.2. Validación para la renovación de certificados tras la revocación

No se podrán renovar certificados que hayan sido revocados en ningún caso, debiéndose proceder a una nueva solicitud y validación de la identidad, de acuerdo con lo establecido en la sección 3.2.

3.4. Identificación y autenticación de la solicitud de revocación

La Agencia Notarial de Certificación deberá autenticar las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Dichas peticiones e informes serán confirmados cumpliendo los procedimientos establecidos en la Declaración de Prácticas de Certificación correspondiente, pudiendo consistir en mecanismos de autenticación basados en conocimiento de información previamente suministrada o acordada con la Agencia Notarial de Certificación durante el procedimiento de emisión de los certificados.

4. Requisitos de operación del ciclo de vida de los certificados

4.1. Solicitud de emisión de certificado

4.1.1. Legitimación para solicitar la emisión

Antes de la emisión y entrega de un certificado, debe existir una solicitud de certificado, a instancia de parte interesada.

Las solicitudes pueden realizarse a tres tipos de entidades de registro:

1) Las solicitudes de certificados colegiales, correspondientes a la clase "Consejo General del Notariado" y clase "Corporaciones de Derecho Público" sólo pueden realizarse ante entidades de registro pertenecientes a las corporaciones que corresponda.
2) Las solicitudes de certificados de clase "Notariales" sólo pueden realizarse ante Notario/a colegiado en España.
3) Las solicitudes de certificados de clase "Corporativos" sólo pueden realizarse ante organizaciones privadas que han firmado contrato de entidad de registro con la Agencia Notarial de Certificación.

En caso de que solicitante y suscriptor sean entidades diferentes, como en los certificados colectivos, debe existir una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumentará jurídicamente.

Podrán existir los siguientes tipos de solicitudes:

1) Presolicitud, que consiste en una solicitud, electrónica o presencial, de un certificado (no contiene clave pública, ni se encuentra firmada digitalmente).
2) Solicitud, que se realiza presencialmente, y que en todo caso produce una petición técnica y electrónica de certificado por la entidad de registros, con generación de claves o sobre una clave pública aportada por el solicitante (PKCS#10 o mecanismo compatible, con la clave pública del usuario y su firma digital, al objeto de demostrar la posesión de la clave privada, de acuerdo con la sección 3.2.1 de la presente política de certificado).

La solicitud de certificado debe documentarse, ya sea en papel o en formato electrónico, incluyendo la adhesión del solicitante a las condiciones generales de emisión.

4.1.2. Procedimiento de alta; Responsabilidades

La entidad de registro correspondiente de la Agencia Notarial de Certificación debe asegurarse de que las solicitudes de certificado son completas, precisas y están debidamente autorizadas.

Antes de la emisión y entrega del certificado, la entidad de registro informará al suscriptor o al poseedor de claves, según proceda, de los términos y condiciones aplicables al certificado.

La citada información se comunicará en soporte duradero, en papel o electrónicamente y en lenguaje fácilmente comprensible.

A la solicitud se deberá acompañar la documentación justificativa de la identidad y otras circunstancias del solicitante, del futuro suscriptor y del poseedor de claves, según proceda, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3 de esta política de certificados.

También se deberá acompañar una dirección física, u otros datos, que permitan contactar al solicitante, al futuro suscriptor y al poseedor de claves, según proceda.

4.2. Procesamiento de la solicitud de certificación

4.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, el prestador de servicios de certificación debe verificar la información proporcionada, conforme a la sección 3.2 de esta política y cumpliendo con los requisitos concretos establecidos para cada certificado en la correspondiente política específica.

4.2.2. Aprobación o rechazo de la solicitud

Si la verificación no es correcta, o si se sospecha que no es correcta, la entidad de registro debe denegar la petición, o detener su aprobación hasta haber realizado las comprobaciones oportunas.

En caso de que los datos se verifiquen correctamente, la Agencia Notarial de Certificación deberá aprobar la solicitud del certificado.

La Agencia Notarial de Certificación deberá notificar al solicitante la aprobación o denegación de la solicitud.

4.2.3. Plazo para resolver la solicitud

Sin estipulación.

4.3. Emisión del certificado

4.3.1. Acciones durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procederá a la emisión del certificado y grabación en el dispositivo cualificado, de forma segura y se entregará la misma al solicitante para su aceptación, de acuerdo con lo establecido en la sección 4.3.2.

La Agencia Notarial de Certificación deberá:

- Emplear un procedimiento de generación de certificados que vincule de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Proteger la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados electrónicamente con el solicitante, durante la presolicitud.
- Incluir en el certificado las informaciones establecidas en el Anexo I del Reglamento (UE) 910/2014, de acuerdo con lo establecido en las secciones 3.1 y 7.1 de esta política.

- Indicar la fecha y la hora en que se expidió un certificado.
- En los casos en que la Agencia Notarial de Certificación aporta el dispositivo cualificado de creación de firma, emplear un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al solicitante, el suscriptor al poseedor de claves, según proceda.
- 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.
- Asegurarse de que el certificado es emitido por sistemas que utilicen protección contra falsificación y, en caso de que el prestador de servicios de certificación genere claves privadas, que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.

4.3.2. Notificación de la emisión al suscriptor

La Agencia Notarial de Certificación notificará, en el acto de emisión o posteriormente, la emisión del certificado al suscriptor o, en su caso, al poseedor de claves.

En certificados de sistemas o certificados de otros tipos emitidos a claves generadas en dispositivos seguros que estuvieran previamente en poder del solicitante, se notificará que el certificado se encuentra disponible y el modo de obtenerlo.

4.4. Entrega y aceptación del certificado

4.4.1. Responsabilidades de la Agencia Notarial de Certificación

- Proporcionar al suscriptor o al poseedor de claves, acceso al certificado, entregando, en su caso, el dispositivo cualificado.
- Entregar al poseedor de claves una hoja de entrega del certificado y, en su caso, del dispositivo, con los siguientes contenidos mínimos:

  a) Información básica acerca de la política y uso del certificado, incluyendo especialmente información acerca de la Agencia Notarial de Certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades

  b) Información acerca del certificado y del dispositivo cualificado, según proceda.

  c) Reconocimiento por parte de suscriptor o poseedor de claves, según proceda, de recibir el certificado y, en su caso, el dispositivo cualificado, y aceptación de los citados elementos.

  d) Obligaciones del suscriptor y, en su caso, del poseedor de claves.

  e) Responsabilidad del suscriptor y, en su caso, del poseedor de claves.

f) Método de imputación exclusiva al suscriptor y, en su caso, al poseedor, de su clave privada y de sus datos de activación del certificado y, cuando proceda, del dispositivo cualificado, de acuerdo con lo establecido en las secciones 6.2 y 6.4 de esta política.

g) La fecha del acto de entrega y aceptación.

4.4.2. Conducta que constituye aceptación del certificado

La Agencia Notarial de Certificación documentará en su Declaración de Prácticas de Certificación y en su documentación jurídica, la(s) conducta(s) que constituya(n) aceptación del certificado.

4.4.3. Publicación del certificado

La Agencia Notarial de Certificación publicará el certificado en el Depósito a que se refiere la sección 2.1 de esta política, con los controles de acceso pertinentes.

4.4.4. Notificación de la emisión a terceros

La Agencia Notarial de Certificación podrá establecer casos y métodos en que se notifique la emisión a terceros.

4.5. Uso del par de claves y del certificado

4.5.1. Uso por el suscriptor y, en su caso, poseedor de claves

4.5.1.1. Obligaciones del suscriptor y en su caso, poseedor de claves

La Agencia Notarial de Certificación obligará al suscriptor, mediante las condiciones generales de emisión, a:

- En caso que el suscriptor genere sus propias claves, se le deberá obligar a:

  a) Generar sus claves de suscriptor empleando un algoritmo reconocido como aceptable para la firma electrónica cualificada.

  b) Crear las claves dentro del dispositivo cualificado de creación de firma

  c) Emplear longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica cualificada.

- Facilitar a la Agencia Notarial de Certificación y a sus entidades de registro información completa y adecuada, conforme a los requerimientos de esta política de certificado y de las políticas específicas, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado, así como a su publicación en el Depósito y cuando, proceda, a la notificación de la emisión a terceros.
- Cumplir las obligaciones que se establecen para el suscriptor en la presente política de certificación y en las políticas específicas.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4 de esta política y en las políticas específicas.

- Ser diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4 de la presente política de certificación y en las políticas específicas, no cediendo el uso de la clave privada a ninguna otra persona.
- Comunicar a la Agencia Notarial de Certificación y a cualquier persona que el suscriptor o el poseedor de claves crea que pueda confiar en el certificado, sin retrasos injustificables:

  a) La pérdida, el robo o el compromiso potencial de su clave privada o del dispositivo cualificado.

  b) La pérdida de control sobre su clave privada o del dispositivo cualificado, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo cualificado de creación de firma) o por cualquier otra causa.

  c) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor o el poseedor de claves.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2 de esta política y en las políticas específicas.
- Transferir a los poseedores de claves las obligaciones específicas de los mismos.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.

El suscriptor del certificado de firma electrónica que genere firmas digitales empleando la clave privada correspondiente a su clave pública listada en el certificado, deberá reconocer, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, conforme a lo establecido en el artículo 25 del Reglamento (UE) 910/2014.

4.5.1.2. Responsabilidad civil del suscriptor de certificado

4.5.1.2.1. Garantías ofrecidas por el suscriptor

La Agencia Notarial de Certificación deberá obligar al suscriptor y, en su caso, al poseedor de claves, mediante las condiciones generales de emisión, a garantizar:

- En caso de que el suscriptor fuese el solicitante del certificado, que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación correspondiente.

- Que cada firma digital creada empleando la clave pública listada en el certificado es la firma digital del suscriptor y que el certificado ha sido aceptado y se encuentra operativo (no ha expirado ni ha sido revocado) en el momento de creación de la firma.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni a título de prestador de servicios de certificación ni en ningún otro caso.
- Que sólo creará firmas digitales mientras tenga la seguridad que ninguna persona no autorizada ha tenido jamás acceso a su clave privada.

4.5.1.2.2. Protección de la clave privada

La Agencia Notarial de Certificación deberá obligar al suscriptor, mediante las condiciones generales de emisión, a garantizar que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.

4.5.2. Uso por el tercero que confía en certificados

4.5.2.1. Obligaciones del tercero que confía en certificados

4.5.2.1.1. Régimen general

La Agencia Notarial de Certificación debe obligar al tercero que confía en certificados, mediante las condiciones generales de uso, a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez, suspensión o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.
- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Agencia Notarial de Certificación ni del Consejo General del Notariado, sin permiso previo por escrito.

4.5.2.1.2. Certificado de firma electrónica

La Agencia Notarial de Certificación deberá obligar al tercero, mediante las condiciones generales de uso, a reconocer que las firmas electrónicas válidamente verificadas con los certificados son firmas electrónicas equivalentes a firmas manuscritas, de acuerdo con el artículo 25 del Reglamento (UE) 910/2014.

4.5.2.2. Responsabilidad civil del tercero que confía en certificados

El prestador de servicios de certificación deberá obligar al tercero que confía en el certificado, mediante las condiciones generales de uso, a reconocer:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6. Renovación de certificados

Los certificados vigentes se podrán renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación.

La renovación de los certificados se podrá realizar con o sin la renovación de las claves, de acuerdo con lo establecido en la sección 4.7 de esta política.

Los certificados podrán ser renovados durante su periodo de vigencia (en función de lo establecido en la DPC correspondiente).

4.7. Renovación de claves y certificados

4.7.1. Causas de renovación de claves y certificados

Los certificados podrán renovarse (en función de lo establecido en la DPC correspondiente), conjuntamente con las claves cuando se llegue al final del periodo de vida de las mismas, o del periodo de vida del dispositivo cualificado en que se contengan.

4.7.2. Legitimación para solicitar la renovación

Antes de la emisión y entrega de un certificado renovado, debe existir una solicitud de renovación de certificado, que debe producirse a instancia del suscriptor o del poseedor de claves, según proceda.

4.7.3. Procesamiento de la solicitud de renovación

La solicitud de renovación será realizada y enviada por el suscriptor o el poseedor de claves, con su certificado vigente, como prueba de posesión de clave privada.

En caso que la información a incluir en el certificado renovado no haya cambiado, incluyendo la información de contacto, se emitirá y entregará automáticamente un nuevo certificado.

La Agencia Notarial de Certificación deberá realizar una confirmación posterior de la identidad del poseedor de claves, de acuerdo con los procedimientos previstos para la validación inicial de la identidad.

En caso de renovación de certificados que hayan expirado o hayan sido revocados, no se procederá a la renovación automática, y deberán realizarse todos los procedimientos de emisión de un certificado nuevo.

4.7.4. Notificación de la emisión del certificado renovado

La Agencia Notarial de Certificación notificará la emisión del certificado al suscriptor y al poseedor de claves, según proceda.

4.7.5. Conducta que constituye aceptación del certificado

La aceptación del certificado se producirá como establece la sección 4.4.2 de esta política.

4.7.6. Publicación del certificado

La Agencia Notarial de Certificación publicará el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.7. Notificación de la emisión a terceros

La Agencia Notarial de Certificación podrá establecer casos y métodos en que se notifique la emisión a terceros.

4.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considerará renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1 a 4.4.

4.9. Revocación y suspensión de certificados

La Agencia Notarial de Certificación deberá detallar en la Declaración de Prácticas de Certificación correspondiente los siguientes aspectos:

- Quién puede solicitar la revocación.
- Cómo se remitirá la solicitud.
- Los requisitos de confirmación de solicitudes de revocación.
- Si se pueden suspender certificados, y las causas de suspensión.
- Los mecanismos empleados para distribuir información de estado de revocación.

- El máximo retraso entre la recepción de la solicitud y la disponibilidad por terceros que confían en certificados del cambio del estado de revocación, que no podrá superar en ningún caso el plazo de un día.

4.9.1. Causas de revocación de certificados

Un prestador de servicios de certificación podrá revocar un certificado debido, por lo menos, a las siguientes causas:

1) Circunstancias que afectan a la información contenida en el certificado:

a) Modificación de alguno de los datos contenidos en el certificado.

b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:

a) Compromiso de la clave privada o de la infraestructura o sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por el prestador de servicios de certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en la Declaración de Prácticas de Certificación del prestador de servicios de certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado del suscriptor o del poseedor de claves.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada del suscriptor o del poseedor de claves.

e) El uso irregular del certificado por el suscriptor o del poseedor de claves, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan a la seguridad del dispositivo criptográfico:

a) Compromiso o sospecha de compromiso de la seguridad del dispositivo criptográfico.

b) Pérdida o inutilización por daños del dispositivo criptográfico.

c) Acceso no autorizado, por un tercero, a los datos de activación del suscriptor o del poseedor de claves.

4) Circunstancias que afectan al suscriptor o al poseedor de claves:

a) Finalización de la relación jurídica entre el prestador de servicios de certificación y el suscriptor o del poseedor de claves.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado al suscriptor o del poseedor de claves.

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

d) Infracción por el suscriptor o del poseedor de claves, de sus obligaciones, responsabilidad y garantías, establecidas en las condiciones generales de emisión correspondientes o en la Declaración de Prácticas de Certificación aplicable.

e) La incapacidad sobrevenida o el fallecimiento del suscriptor o del poseedor de claves.

f) En caso de certificados de colectivo, la extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y poseedor de claves.

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4 de esta política.

5) Otras circunstancias:

a) La suspensión del certificado digital por un período superior al establecido en la sección 4.9.13 de esta política.

b) La terminación del servicio por la Agencia Notarial de Certificación, de acuerdo con lo establecido en la sección 5.8 de esta política.

La Agencia Notarial de Certificación podrá establecer en las políticas específicas otras causas de revocación, siempre que resulten compatibles con el ordenamiento jurídico y, en concreto, con el Reglamento (UE) 910/2014.

Asimismo, cada Declaración de Prácticas de Certificación deberá adaptar las causas anteriores a cada caso concreto.

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

En este caso se considerará que las actuaciones realizadas durante el período de suspensión no son válidas, siempre y cuando el certificado finalmente sea revocado. Serán válidas si se levanta la suspensión y el certificado vuelve a pasar a la situación de válido.

Las condiciones generales de emisión deberán establecer la obligación de solicitar la revocación del certificado en caso de tener conocimiento de alguna de las circunstancias anteriormente indicadas.

4.9.2. Legitimación para solicitar la revocación

Podrán solicitar la revocación de un certificado:

- El suscriptor a nombre del cual el certificado fue emitido.
- En caso de certificados corporativos y de colectivo, un representante autorizado por el suscriptor, o el propio poseedor de claves.

- En caso de certificados de representación, el representado.
- La entidad de registro que solicitó la emisión del certificado, o cualquier otra que reciba una solicitud de revocación.

4.9.3. Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a la Agencia Notarial de Certificación o, en su caso, a cualquier entidad de registro de las autorizadas para cada política específica de certificado, comprensiva de la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

En aquellos casos en que se requiera revocación inmediata del certificado, se podrá hacer una llamada o enviar un correo electrónico a la Agencia Notarial de Certificación.

La solicitud debe ser autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

En caso de que el destinatario de la solicitud fuera una entidad de registro, una vez autenticada, podrá revocar directamente el certificado o remitir una solicitud en este sentido a la Agencia Notarial de Certificación, dependiendo de lo establecido en la política específica de certificado.

La solicitud de certificación será procesada a su recepción.

Se deberá informar al suscriptor y, en su caso, al poseedor de claves, acerca del cambio de estado del certificado revocado.

La Agencia Notarial de Certificación no podrá reactivar el certificado, una vez revocado.

4.9.4. Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma razonablemente inmediata en cuanto se tenga conocimiento de la causa de revocación.

4.9.5. Obligación de consulta de información de revocación de certificados

Los terceros que confían en certificados deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Entidad de Certificación que emitió el certificado en el cual se desea confiar.

La Agencia Notarial de Certificación deberá suministrar información a los terceros que confían en certificados acerca de cómo y dónde encontrar la Lista de Revocación de Certificados correspondiente.

4.9.6. Frecuencia de emisión de listas de revocación de certificados (CRLs)

La Agencia Notarial de Certificación deberá emitir una nueva CRL al menos cada 24 horas. Adicionalmente, deberá emitir una nueva CRL en un tiempo razonable después de la revocación de un certificado.

Se deberá indicar en la CRL el momento programado de emisión de una nueva CRL, si bien se podrá emitir una CRL antes del plazo indicado en la CRL anterior.

Los certificados revocados que expiren podrán ser retirados de la CRL.

4.9.7. Disponibilidad de servicios de comprobación de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar su estado en el Depósito de certificados de la Agencia Notarial de Certificación, que deberá estar disponible las 24 horas de los 7 días de la semana.

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Agencia Notarial de Certificación, ésta deberá realizar sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible.

La Declaración de Prácticas de Certificación deberá suministrar información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Obligación de consulta de servicios de comprobación de estado de certificados

El tercero que confía en el certificado que no emplee CRLs para comprobar la validez de un certificado, deberá emplear el Depósito para ello.

4.9.8. Otras formas de información de revocación de certificados

La Agencia Notarial de Certificación podrá implantar otras formas de provisión de información acerca del estado de revocación de los certificados, debiendo describir las provisiones correspondientes a su funcionamiento en su Declaración de Prácticas de Certificación.

En concreto, se deberá disponer de un servicio OCSP público para suministrar información de estado.

4.9.9. Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de una Entidad de Certificación será notificado, en la medida de lo posible, a todos los participantes en los servicios de certificación del Consejo General del Notariado y la Agencia Notarial de Certificación.

Se detallará en la Declaración de Prácticas de Certificación el modo en que se dará cumplimiento a esta obligación.

4.9.10. Causas de suspensión de certificados

La Agencia Notarial de Certificación podrá suspender certificados en los siguientes casos:

- La simple solicitud.
- Resolución judicial o administrativa que lo ordene, o la existencia de una investigación o procedimiento judicial o administrativo que pudiera determinar que el certificado está afectado por una causa de revocación.
- La existencia de dudas fundadas acerca de la concurrencia de las causas de revocación de los certificados.

Debe asegurarse de que el certificado no está suspendido durante más tiempo del necesario para confirmar las causas anteriores.

4.9.11. Legitimación para solicitar la suspensión

Podrán solicitar la suspensión de un certificado el suscriptor, la persona física o jurídica representada por éste o un tercero autorizado.

4.9.12. Procedimientos de petición de suspensión

Para proceder a una solicitud electrónica de suspensión, el suscriptor o, en su caso el poseedor de claves, deberá telefonear a un teléfono de la Agencia Notarial de Certificación, que grabará y almacenará la solicitud.

El solicitante de la suspensión deberá responder con la contraseña o secreto compartido indicado por el mismo durante el proceso de solicitud del certificado. En caso de que la respuesta coincida con dicha contraseña se procederá a suspender el certificado.

Se determinarán en la Declaración de Prácticas de Certificación los procedimientos y mecanismos de acceso a los sistemas de suspensión.

4.9.13. Plazo máximo de suspensión

El plazo máximo de suspensión será de sesenta (60) días naturales.

4.10. Servicios de comprobación de estado de certificados

4.10.1. Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestarán mediante una interfaz de consulta web, a través del Depósito de los certificados, y a través del servicio OCSP.

4.10.2. Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encontrarán disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.10.3. Características opcionales

Sin estipulación.

4.11. Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio, expirando el certificado.

Como excepción, el suscriptor podrá mantener el servicio vigente, solicitando la renovación del certificado, en los casos y con la antelación que determine esta política y la Declaración de Prácticas de Certificación correspondiente.

4.12. Depósito y recuperación de claves

4.12.1. Política y prácticas de depósito y recuperación de claves

La Agencia Notarial de Certificación no depositará ni podrá recuperar claves de suscriptores o poseedores de claves, excepto para claves de cifrado.

4.12.2. Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5. Controles de seguridad física, de gestión y de operaciones

5.1. Controles de seguridad física

La Agencia Notarial de Certificación debe disponer de instalaciones que protejan físicamente la prestación de, al menos, los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos.

La protección física se logrará mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación. La parte de las instalaciones compartida con otras organizaciones debe encontrarse fuera de estos perímetros.

La Agencia Notarial de Certificación establecerá controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones.

La política de seguridad física y ambiental aplicable a los servicios de generación de certificados, de dispositivos criptográficos y de gestión de revocación deberá establecer prescripciones para

las siguientes contingencias, que se documentarán sucintamente en la Declaración de Prácticas de Certificación:

- Controles de acceso físico.
- Protección frente a desastres naturales.
- Medidas de protección frente a incendios.
- Fallo de los sistemas de apoyo (energía electrónica, telecomunicaciones, etc.)
- Derrumbamiento de la estructura.
- Inundaciones.
- Protección antirrobos.
- Allanamiento y entrada no autorizada.
- Recuperación del desastre.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

5.1.1. Localización y construcción de las instalaciones

La localización de las instalaciones debe permitir la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos (en el caso de no contar con presencia física permanente de personal de seguridad del prestador de servicios de certificación)

La calidad y solidez de los materiales de construcción de las instalaciones deberá garantizar unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

5.1.2. Acceso físico

La Agencia Notarial de Certificación deberá establecer al menos cuatro (4) niveles de seguridad con restricción de acceso a los diferentes perímetros y barreras físicas definidas.

Para el acceso a las dependencias del prestador de servicios de certificación donde se lleven a cabo procesos relacionados con el ciclo de vida del certificado, será necesaria la autorización previa, identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.

Esta identificación, ante el sistema de control de accesos, deberá realizarse mediante reconocimiento de algún parámetro biométrico del individuo, excepto en caso de visitas escoltadas.

La generación de claves criptográficas de las Entidades de Certificación, así como su almacenamiento, deberá realizarse en dependencias específicas para estos fines, y requerirán de acceso y permanencia duales.

5.1.3. Electricidad y aire acondicionado

Los equipos informáticos del prestador de servicios de certificación deberán estar convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

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

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

5.1.4. Exposición al agua

La Agencia Notarial de Certificación deberá disponer de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad, en el caso de que las condiciones de ubicación de las instalaciones lo hagan necesario.

5.1.5. Prevención y protección de incendios

Todas las instalaciones y activos de la Agencia Notarial de Certificación deben contar con sistemas automáticos de detección y extinción de incendios.

En concreto, los dispositivos criptográficos, y soportes que almacenen claves de los prestadores de servicios de certificación, deberán contar con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

5.1.6. Almacenamiento de soportes

El almacenamiento de soportes de información debe realizarse de forma que se garantice tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se haya establecido.

Deberá contarse para ellos con dependencias o armarios ignífugos.

El acceso a estos soportes, incluso para su eliminación, deberá estar restringido a personas específicamente autorizadas.

5.1.7. Tratamiento de residuos

La eliminación de soportes, tanto papel como magnéticos, se deberá realizar mediante mecanismos que garanticen la imposibilidad de recuperación de la información.

En el caso de soportes magnéticos, se procederá al formateo, borrado permanente, o destrucción física del soporte.

En el caso de documentación en papel, éste deberá someterse a un tratamiento físico de destrucción.

5.1.8. Copia de respaldo fuera de las instalaciones

Periódicamente, la Agencia Notarial de Certificación almacenará copia de respaldo de los sistemas de información, en dependencias físicamente separadas de aquellas en las que se encuentran los equipos.

5.2. Controles de procedimientos

La Agencia Notarial de Certificación debe garantizar que sus sistemas se operan de forma segura, para lo cual deberá establecer e implantar procedimientos para las funciones que afecten a la provisión de sus servicios.

El personal al servicio de la Agencia Notarial de Certificación realizará los procedimientos administrativos y de gestión de acuerdo con la política de seguridad establecida.

5.2.1. Funciones fiables

La Agencia Notarial de Certificación deberá identificar, en su política de seguridad, funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos deberán ser formalmente nombrados por la alta dirección del prestador de servicios de certificación.

Las funciones fiables deberán incluir:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Auditores del sistema.

5.2.2. Número de personas por tarea

Las funciones fiables identificadas en la sección anterior y en la política de seguridad, y sus responsabilidades asociadas, serán documentadas en descripciones de puestos de trabajo, y descritas de forma sucinta en la Declaración de Prácticas de Certificación correspondiente.

Dichas descripciones deberán realizarse teniendo en cuenta que debe existir una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

Para determinar la sensibilidad de la función, se tendrán en cuenta los siguientes elementos:

- Deberes asociados a la función.
- Nivel de acceso.
- Monitorización de la función.
- Formación y concienciación.
- Habilidades requeridas.

5.2.3. Identificación y autenticación para cada función

La Agencia Notarial de Certificación deberá identificar y autenticar al personal antes de acceder a la correspondiente función fiable.

5.2.4. Roles que requieren separación de tareas

Las siguientes tareas deberán ser realizadas, al menos, por dos personas:

- Gestión del acceso físico.
- Gestión de aplicaciones informáticas del prestador.
- Gestión de configuración y control de cambios.
- Gestión del archivo.
- Gestión de bienes de equipo criptográfico.
- Generación de certificados de autoridad de certificación.

5.3. Controles de personal

5.3.1. Requisitos de historial, calificaciones, experiencia y autorización

La Agencia Notarial de Certificación deberá emplear personal cualificado y con la experiencia necesaria, para la prestación de los servicios ofrecidos, en el ámbito de la firma electrónica y los procedimientos de seguridad y de gestión adecuados.

Este requisito se aplicará al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

La calificación y la experiencia podrán suplirse mediante una formación y entrenamiento apropiados.

El personal en puestos fiables deberá encontrarse libre de intereses personales que entre en conflicto con el desarrollo de la función que tenga encomendada.

No se podrá asignar a un puesto fiable o de gestión a una persona que no sea idóneo para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se deberá realizar una investigación, de acuerdo con lo establecido en la sección siguiente, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación de que realmente se hizo el trabajo alegado.
- Morosidad.
- Hasta donde lo permite la legislación vigente, antecedentes penales.

5.3.2. Procedimientos de investigación de historial

La Agencia Notarial de Certificación deberá realizar la investigación antes de que la persona sea contratada y/o acceda al puesto de trabajo.

En la solicitud para el puesto de trabajo se informará acerca de la necesidad de someterse a una investigación previa.

Se deberá advertir de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

Se deberá obtener consentimiento inequívoco del afectado por la investigación previa y procesar y proteger todos sus datos personales de acuerdo con la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales..

La investigación se repetirá cada tres años.

5.3.3. Requisitos de formación

La Agencia Notarial de Certificación deberá formar al personal en puestos fiables y de gestión, hasta que alcancen la calificación necesaria, de acuerdo con lo establecido en la sección 5.3.1 de esta política.

La formación deberá incluir los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Versiones de maquinaria y aplicaciones en uso.
- Tareas que debe realizar la persona.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.

5.3.4. Requisitos y frecuencia de actualización formativa

La Agencia Notarial de Certificación deberá realizar una actualización en la formación del personal al menos cada dos años.

5.3.5. Secuencia y frecuencia de rotación laboral

La Agencia Notarial de Certificación podrá establecer métodos de rotación laboral para la prestación del servicio en turnos, con el objeto de cubrir las necesidades de 24x7 del servicio.

5.3.6. Sanciones para acciones no autorizadas

La Agencia Notarial de Certificación deberá disponer de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que deberá encontrarse adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias podrán incluir la suspensión y el despido de la persona responsable de la acción dañina.

5.3.7. Requisitos de contratación de profesionales

La Agencia Notarial de Certificación podrá contratar profesionales para cualquier función, incluso para un puesto fiable, en cuyo caso deberá someterse a los mismos controles que los restantes empleados.

En el caso de que el profesional no deba someterse a tales controles, deberá estar constantemente acompañado por un empleado fiable, cuando se encuentre en las instalaciones de la Agencia Notarial de Certificación.

5.3.8. Suministro de documentación al personal

La Agencia Notarial de Certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección 5.3.1 de esta política.

5.4. Procedimientos de auditoría de seguridad

5.4.1. Tipos de eventos registrados

La Agencia Notarial de Certificación debe guardar registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado de los sistemas.
- Inicio y terminación de la aplicación de autoridad de certificación o de autoridad de registro central.
- Intentos de crear, borrar, cambiar contraseñas o permisos de los usuarios dentro del sistema.
- Generación y cambios en las claves de la Entidad de Certificación.
- Cambios en las políticas de emisión de certificados.
- Intentos de entrada y salida del sistema.
- Intentos no autorizados de entrada en la red de la Entidad de Certificación.
- Intentos no autorizados de acceso a los ficheros del sistema.
- Intentos fallidos de lectura en un certificado, y de lectura y escritura en el Depósito de certificados.
- Eventos relacionados con el ciclo de vida del certificado, como solicitud, emisión, revocación y renovación de un certificado.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como recepción, uso y desinstalación del mismo.

La Agencia Notarial de Certificación debe también guardar, ya sea manual o electrónicamente, la siguiente información:

- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Los registros de acceso físico.

- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor o del poseedor de claves.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.

5.4.2. Frecuencia de tratamiento de registros de auditoría

Los registros de auditoría se examinarán por lo menos una vez al mes en busca de actividad sospechosa o no habitual.

El procesamiento de los registros de auditoría consistirá en una revisión de los registros la cual incluye la verificación de que los registros no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros.

Las acciones llevadas a cabo a partir de la revisión de auditoría también deben ser documentadas.

5.4.3. Periodo de conservación de registros de auditoría

Los registros de auditoría se deben retener en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivarán de acuerdo con la sección 5.5.2 de esta política.

5.4.4. Protección de los registros de auditoría

Los ficheros de registros, tanto manuales como electrónicos, deben protegerse de lecturas, modificaciones, borrados o cualquier otro tipo de manipulación no autorizada usando controles de acceso lógico y físico.

5.4.5. Procedimientos de copia de respaldo

Se deberán generar, al menos, copias incrementales de respaldo de registros de auditoría diariamente y copias completas semanalmente.

5.4.6. Localización del sistema de acumulación de registros de auditoría

El sistema de acumulación de registros de auditoría deberá ser, al menos, un sistema interno de la Agencia Notarial de Certificación, compuesto por los registros de la aplicación, por los registros de red y por los registros del sistema operativo, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado.

5.4.7. Notificación del evento de auditoría al causante del evento

Cuando el sistema de acumulación de registros de auditoría registre un evento, no será preciso enviar una notificación al individuo, organización, dispositivo o aplicación que causó el evento.

Se podrá comunicar si el resultado de su acción ha tenido éxito o no, pero no que se ha auditado la acción.

5.4.8. Análisis de vulnerabilidades

Los eventos en el proceso de auditoría deberán ser guardados, en parte, para monitorizar las vulnerabilidades del sistema.

Los análisis de vulnerabilidad deben ser ejecutados, repasados y revisados a través de un examen de esos eventos monitorizados.

Estos análisis deben ser ejecutados diariamente, mensualmente y anualmente de acuerdo con su definición en el plan de auditoría o documento que lo sustituya, de la Agencia Notarial de Certificación.

5.5. Archivo de informaciones

La Agencia Notarial de Certificación debe garantizar que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1. Tipos de eventos registrados

La Agencia Notarial de Certificación debe guardar todos los eventos que tengan lugar durante el ciclo de vida de un certificado, incluyendo la renovación del mismo.

Se debe guardar un registro de lo siguiente:

- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- Identidad de la entidad que procesa la solicitud de certificado.
- La ubicación de las copias de solicitudes de certificados y del documento firmado por el suscriptor o por el poseedor de las claves, según proceda.

5.5.2. Periodo de conservación de registros

La Agencia Notarial de Certificación debe guardar los registros especificados en la sección anterior de esta política de forma permanente, con un mínimo de quince (15) años.

5.5.3. Protección del archivo

La Agencia Notarial de Certificación debe:

- Mantener la integridad y la confidencialidad del archivo que contiene los datos referentes a los certificados emitidos.

- Archivar los datos anteriormente citados de forma completa y confidencial.
- Mantener la privacidad de los datos de registro del suscriptor o del poseedor de las claves, según proceda.

5.5.4. Procedimientos de copia de respaldo

La Agencia Notarial de Certificación debe realizar copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección 5.5.1 de esta política. Debe, además, realizar copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.

Además, debe guardar los documentos en papel, según la sección 5.5.1, en un lugar fuera de las instalaciones de la propia Agencia Notarial de Certificación para casos de recuperación de datos, de acuerdo con la sección 5.7 de esta política.

5.5.5. Requisitos de sellado de fecha y hora

La Agencia Notarial de Certificación debe emitir los certificados y las CRLs con información fiable de fecha y hora.

No será necesario que esta información se encuentre firmada digitalmente.

5.5.6. Localización del sistema de archivo

La Agencia Notarial de Certificación debe disponer de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 5.5.4 de esta política.

5.5.7. Procedimientos de obtención y verificación de información de archivo

Sólo personas autorizadas por la Agencia Notarial de Certificación podrán tener acceso a los datos de archivo, ya sea en las mismas instalaciones de la Agencia Notarial de Certificación o en su ubicación externa.

5.6. Renovación de claves

La Agencia Notarial de Certificación deberá establecer un plan de renovación programada de las claves de los certificados de infraestructura, que garantice la continuidad de los servicios.

5.7. Compromiso de claves y recuperación de desastre

5.7.1. Corrupción de recursos, aplicaciones o datos

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, la Agencia Notarial de Certificación debe iniciar las gestiones necesarias, de acuerdo con el plan de seguridad, el plan de emergencia y el plan de auditoría, o documentos que los sustituyan, para hacer que el sistema vuelva a su estado normal de funcionamiento.

5.7.2. Revocación de la clave pública de la entidad

En el caso de que la Agencia Notarial de Certificación deba revocar la clave pública de una Entidad de Certificación de su jerarquía, deberá llevar a cabo lo siguiente:

- Notificar este hecho, cuando se produzca, al Consejo General del Notariado.
- Informar del hecho publicando una CRL, según lo establecido en la sección 4.9.6 de esta política.
- Realizar todos los esfuerzos necesarios para informar de la revocación a todos los suscriptores a los cuales la Agencia Notarial de Certificación haya emitido certificados, así como a los terceros que confían en certificados que deseen confiar en esos certificados.
- Realizar una renovación de claves, en caso de que la revocación no haya sido debida a la terminación del servicio por parte de la Agencia Notarial de Certificación acreditado, según lo establecido en la sección 5.6 de esta política.

5.7.3. Compromiso de la clave privada de la entidad

El plan de continuidad de negocio de la Agencia Notarial de Certificación (o plan de recuperación de desastres) debe considerar el compromiso o la sospecha de compromiso de la clave privada de las Entidades de Certificación como un desastre.

En caso de compromiso, la Agencia Notarial de Certificación debe realizar como mínimo las siguientes acciones:

- Informar a todos los suscriptores y terceros del compromiso.
- Indicar que los certificados y la información del estado de revocación que han sido entregados usando la clave de esta Entidad de Certificación ya no son válidos.

5.7.4. Desastre sobre las instalaciones

La Agencia Notarial de Certificación debe desarrollar, mantener, probar y, si es necesario, ejecutar un plan de emergencia para el caso de que ocurra un desastre, ya sea por causas naturales o causado por el hombre, sobre las instalaciones, el cual indique cómo restaurar los servicios de los sistemas de información.

La Agencia Notarial de Certificación debe restaurar los servicios críticos dentro de las 24 horas siguientes al desastre. Estos servicios son los siguientes:

- Revocación de certificados.
- Publicación de información de revocación de los certificados.

La ubicación de los sistemas de recuperación de desastres debe disponer de las protecciones físicas de seguridad detalladas en el plan de seguridad.

La base de datos de recuperación de desastres utilizada por la Agencia Notarial de Certificación debe estar sincronizada con la base de datos de producción, dentro de los límites temporales especificados en el plan de seguridad.

Los equipos de recuperación de desastres deben tener las medidas de seguridad físicas especificadas en el plan de seguridad, equivalentes a las de las instalaciones principales.

5.8. Terminación del servicio

La Agencia Notarial de Certificación debe asegurar que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios de la Entidad de Certificación y, en particular, asegurar un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal.

Antes de terminar sus servicios, la Agencia Notarial de Certificación debe ejecutar, como mínimo, los siguientes procedimientos:

- Informar a todos los suscriptores y terceros que confían en certificados.
- Retirar toda autorización de subcontrataciones que actúan en su nombre en el proceso de emisión de certificados.
- Ejecutar las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.
- Destruir las claves privadas de la Entidad de Certificación o retirarlas de su uso.

La Agencia Notarial de Certificación debe declarar en sus prácticas las previsiones que tiene para el caso de terminación del servicio. Estas deben incluir:

- Notificación a las entidades afectadas.
- Transferencia de sus obligaciones a otras personas.
- Cómo se tratará el estado de revocación de los certificados emitidos que aún no han expirado.

6. Controles de seguridad técnica

La Agencia Notarial de Certificación deberá emplear sistemas y productos fiables, que estén protegidos contra toda alteración y que garanticen la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1. Generación e instalación del par de claves

6.1.1. Generación del par de claves

La Agencia Notarial de Certificación, cuando actúe como Entidad de Certificación raíz, generará y firmará su propio par de claves y procederá a la generación de las claves de cada Entidad de Certificación subordinada, todo ello de acuerdo con la ceremonia de claves, dentro del perímetro de alta seguridad destinado específicamente a esta tarea.

Los pares de claves de las Entidades de Certificación (raíz o subordinadas) deben ser generados empleando hardware criptográfico que cumpla ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en EN 419 221-5; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

Los pares de claves de los suscriptores y de los operadores y administradores de las entidades de registro, deberán generarse siempre en dispositivos criptográficos que cumplan ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en EN 419 211 partes 1 a 5, según proceda; o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes, excepto en el caso de los certificados de firma electrónica avanzada o de los certificados de sistemas.

Dichos dispositivos seguros podrán ser tarjetas criptográficas, tokens USB criptográficos, o cualquier otro tipo de dispositivo, en especial maquinaria de seguridad (HSM), que cumpla con los requisitos de seguridad establecidos por la normativa vigente para los dispositivos seguros.

La Agencia Notarial de Certificación monitoriza y verifica que los dispositivos de creación de firma se encuentran certificados como dispositivos cualificados de creación de firma (QSCD) en el momento de la emisión. Así mismo, si durante el periodo de validez del certificado electrónico el dispositivo que almacena sus claves pierde su cualificación, se procederá a la revocación del certificado electrónico y se informará al subscriptor del procedimiento para la emisión de un nuevo certificado en un soporte cualificado.

6.1.2. Envío de la clave privada al suscriptor

La clave privada del suscriptor o del poseedor de claves, deberá serle entregada debidamente protegida mediante un dispositivo criptográfico que cumpla lo establecido en ISO 15408: EAL 4 + (o superior), de acuerdo con lo establecido en EN 419 211 o criterios de seguridad equivalentes, excepto en el caso de los certificados de firma electrónica avanzada, sellos electrónicos, firma a distancia o de los certificados de sistemas.

6.1.3. Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública a la Entidad de Certificación será PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la Agencia Notarial de Certificación.

6.1.4. Distribución de la clave pública del prestador de servicios de certificación

Las claves de las Entidades de Certificación deben ser comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen.

La clave pública de cada Entidad de Certificación se publicará en el Depósito, en forma de certificado autofirmado o firmado por otra Entidad de Certificación, junto a una declaración referente a que la clave autentica a la Entidad de Certificación.

Se deberán establecer medidas adicionales para confiar en los certificados autofirmados, como la comprobación de la huella digital del certificado.

Los usuarios podrán acceder al Depósito para obtener las claves públicas de las Entidades de Certificación.

Adicionalmente, en aplicaciones S/MIME, el mensaje de datos podrá contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

6.1.5. Tamaños de claves

La longitud de las claves RSA de las Entidades de Certificación será al menos de 4096 bits, mientras que la de los restantes tipos de certificados será de al menos 2048 bits.

6.1.6. Generación de parámetros de clave pública

Sin estipulación.

6.1.7. Comprobación de calidad de parámetros de clave pública

La Agencia Notarial de Certificación podrá establecer métodos de comprobación de la calidad de los parámetros de las claves públicas.

6.1.8. Generación de claves en aplicaciones informáticas o en bienes de equipo

Las claves de las Entidades de Certificación se generarán en hardware criptográfico que cumpla el estándar ISO 15408: EAL 4 (o superior), de acuerdo con lo dispuesto en EN 419221-5, o FIPS 140-2 Nivel 3 (o superior), o criterios de seguridad equivalentes.

Las claves de firma electrónica cualificada de los usuarios finales se generarán en dispositivos criptográficos que cumplan el estándar ISO 15408: EAL 4 (o superior), de acuerdo con lo establecido en EN 419 211, o criterios de seguridad equivalentes.

6.1.9. Propósitos de uso de claves

La Agencia Notarial de Certificación deberá incluir la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas.

6.2. Protección de la clave privada

6.2.1. Estándares de módulos criptográficos

Para los módulos que gestionan claves de las Entidades de Certificación y de los suscriptores de certificados de firma electrónica cualificada, se deberá asegurar el nivel exigido por los estándares indicados en las secciones anteriores.

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

El acceso a las claves privadas de las Entidades de Certificación, se deberá requerir necesariamente del concurso simultáneo de dos (2) dispositivos criptográficos protegidos por una clave de acceso, de entre cuatro (4) dispositivos.

La clave de acceso será conocida únicamente por una persona responsable de ese dispositivo. Ninguna de ellas conocerá más que una de las claves de acceso.

Los dispositivos criptográficos quedarán almacenados en las dependencias del prestador de servicios de certificación, y para su acceso será necesaria una persona adicional.

6.2.3. Custodia de la clave privada

Únicamente se podrán custodiar copias de respaldo de las claves privadas de los certificados de entidad final cuyo uso exclusivo sea el cifrado.

No se custodian otras claves privadas de los suscriptores.

6.2.4. Copia de respaldo de la clave privada

La clave privada de las Entidades de Certificación deberá contar con una copia de respaldo realizada, almacenada en dependencia independiente de aquélla donde se almacena habitualmente, y recuperada en su caso, por personal sujeto a la política de confianza del personal. Este personal debe ser expresamente autorizado a estos fines, y debe limitarse a aquel que necesite hacerlo.

Los controles de seguridad a aplicar a las copias de respaldo de las Entidades de Certificación deberán ser de igual o superior nivel a los que se aplican a las claves habitualmente en uso.

Cuando las claves se almacenen en un módulo hardware de proceso dedicado, deberán proveerse los controles oportunos para que éstas nunca puedan abandonar el dispositivo.

6.2.5. Archivo de la clave privada

Las claves privadas de las Entidades de Certificación serán archivadas al final de su periodo de operación, de forma permanente.

No se archivarán claves privadas de firma electrónica de usuarios finales.

6.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se podrán generar directamente en los módulos criptográficos o en módulos criptográficos externos, de los que se exportarán las claves cifradas para su introducción en los módulos de producción.

Las claves privadas de las Entidades de Certificación quedarán almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no podrán ser extraídas)

Dichos dispositivos serán empleados para introducir la clave privada en el módulo criptográfico.

6.2.7. Método de activación de la clave privada

La clave privada de cada Entidad de certificación se activará mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.

La clave privada del suscriptor se activará mediante la introducción del PIN en el dispositivo criptográfico o aplicación de firma.

6.2.8. Método de desactivación de la clave privada

Para certificados de firma electrónica cualificada, cuando se retire el dispositivo criptográfico del lector o se desconecte del ordenador, o la aplicación que lo utilice finalice la sesión, será necesaria nuevamente la introducción del PIN.

6.2.9. Método de destrucción de la clave privada

Las claves privadas serán destruidas en una forma que impida su robo, modificación, divulgación no autorizada o uso no autorizado.

6.3. Otros aspectos de gestión del par de claves

6.3.1. Archivo de la clave pública

Las Entidades de Certificación archivarán sus claves públicas de forma permanente, de acuerdo con lo establecido en la sección 5.5 de esta política.

6.3.2. Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves serán los determinados por la duración del certificado, transcurrido el cual no podrán continuar utilizándose.

Como excepción, la clave privada podrá continuar empleándose para el descifrado de documentos, incluso tras la expiración del certificado.

6.4. Datos de activación

6.4.1. Generación e instalación de datos de activación

En los casos en que la Agencia Notarial de Certificación facilita al suscriptor un dispositivo cualificado de creación de firma, entonces los datos de activación del dispositivo, deben ser generados de forma segura por el prestador de servicios de certificación.

6.4.2. Protección de datos de activación

La Agencia Notarial de Certificación podrá generar y facilitar al suscriptor los datos de activación del dispositivo cualificado de creación de firma empleando procedimientos seguros, como la entrega presencial o a distancia, en cuyo caso los datos de activación deberán ser distribuidos separadamente del propio dispositivo de creación de firma (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes).

6.4.3. Otros aspectos de los datos de activación

Sin estipulación.

6.5. Controles de seguridad informática

6.5.1. Requisitos técnicos específicos de seguridad informática

Se deberá garantizar que el acceso los sistemas está limitado a individuos debidamente autorizados. En particular:

- Se debe garantizar una administración efectiva del nivel de acceso de los usuarios (operadores, administradores, así como cualquier usuario con acceso directo al sistema) para mantener la seguridad del sistema, incluyendo gestión de cuentas de usuarios, auditoría y modificaciones o denegación de acceso oportunas.
- Se debe garantizar que el acceso a los sistemas de información y aplicaciones se restringe de acuerdo a lo establecido en la política de control de acceso, así como que los sistemas proporcionan los controles de seguridad suficientes para implementar la segregación de funciones identificada en las prácticas, incluyendo la separación de funciones de administración de los sistemas de seguridad y de los operadores. En concreto, el uso de programas de utilidades del sistema estará restringido y estrechamente controlado.
- El personal deberá ser identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal será responsable y deberá poder justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Deberá evitarse la posibilidad de revelación de datos sensibles mediante la reutilización de objetos de almacenamiento (por ejemplo ficheros borrados) que queden accesibles a usuarios no autorizados.
- Los sistemas de seguridad y monitorización deben permitir una rápida detección, registro y actuación ante intentos de acceso irregular o no autorizado a sus recursos (por ejemplo, mediante sistema de detección de intrusiones, monitorización y alarma)
- El acceso a los depósitos públicos de la información (por ejemplo, certificados o información de estado de revocación) deberá contar con un control de accesos para modificaciones o borrado de datos.

6.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Agencia Notarial de Certificación deberán ser fiables, debiendo acreditarse dicha condición, por ejemplo, mediante una certificación de producto contra un perfil de protección adecuado, conforme a la norma ISO 15408, o equivalente.

6.6. Controles técnicos del ciclo de vida

6.6.1. Controles de desarrollo de sistemas

Se deberá realizar un análisis de requisitos de seguridad durante las fases de diseño y especificación de requisitos de cualquier componente empleado en las aplicaciones de autoridad de certificación y de registro, para garantizar que los sistemas son seguros.

Se emplearán procedimientos de control de cambios para las nuevas versiones, actualizaciones y parches de emergencia, de dichos componentes.

6.6.2. Controles de gestión de seguridad

La Agencia Notarial de Certificación deberá mantener un inventario de todos los activos informativos y realizará una clasificación de los mismos, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se auditará de forma periódica, de acuerdo con lo establecido en la sección 8.1.1 de esta política.

Se realizará un seguimiento de las necesidades de capacidad, y se planificarán procedimientos para garantizar suficiente disponibilidad electrónica y de almacenamiento para los activos informativos.

6.6.3. Evaluación del nivel de seguridad del ciclo de vida

El Consejo General del Notariado podrá exigir que la Agencia Notarial de Certificación se someta a evaluaciones independientes, auditorías y, en su caso, certificaciones de seguridad del ciclo de vida de los productos que emplea.

6.7. Controles de seguridad de red

Se deberá garantizar que el acceso a las diferentes redes de la Agencia Notarial de Certificación está limitado a individuos debidamente autorizados. En particular:

- Deben implementarse controles para proteger la red interna de dominios externos accesibles por terceras partes. Los cortafuegos deberán configurarse de forma que se impidan accesos y protocolos que no sean necesarios para la operación de la Entidad de Certificación.
- Los datos sensibles deberán protegerse cuando se intercambien a través de redes no seguras (incluyendo como tales los datos de registro del suscriptor)
- Se debe garantizar que los componentes locales de red se encuentran ubicados en entornos seguros, así como la auditoría periódica de sus configuraciones.

6.8. Controles de ingeniería de módulos criptográficos

Se debe garantizar que las claves de las Entidades de Certificación son generadas en equipamientos criptográficos, operados por personal de confianza de la Entidad y en un entorno seguro bajo control dual.

Estos equipamientos deben cumplir los estándares criptográficos de seguridad, que se han indicado en las secciones anteriores.

Los algoritmos de generación de claves deberán estar aceptados para el uso de la clave a que esté destinado (para los diferentes tipos de certificados que se definen).

7. Perfiles de certificados y listas de certificados revocados

7.1. Perfil de certificado

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

- Número de serie, que será un código único con respecto al nombre distinguido del emisor
- Algoritmo de firma.
- El nombre distinguido del emisor.
- Inicio de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280
- Fin de validez del certificado, en Tiempo Coordinado Universal, codificado conforme a la RFC 3280
- Nombre distinguido del sujeto.
- Clave pública del sujeto, codificada de acuerdo con RFC 3280
- Firma, generada y codificada de acuerdo con RFC 3280

Los certificados serán conformes con las siguientes normas:

- RFC 3280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile, April 2002
- ITU-T Recommendation X.509 (1997): Information Technology – Open Systems Interconnection - The Directory: Authentication Framework, June 1997, con sus actualizaciones y correcciones posteriores.

Adicionalmente, los certificados de firma electrónica serán conformes con las siguientes normas:

- EN 319 412 : Certificate Profiles.
- RFC 3739: Internet X.509 Public Key Infrastructure – Qualified Certificate Profile, March 2004 (siempre que no entre en conflicto con TS 101 862)

La Agencia Notarial de Certificación publicará sus perfiles de certificados en el Depósito indicado en la sección 2.

7.2. Perfil de la lista de revocación de certificados

La Agencia Notarial de Certificación publicará sus perfiles de listas de revocación de certificados en el Depósito indicado en la sección 2.

8. Auditoría de conformidad

La Agencia Notarial de Certificación debe realizar periódicamente una auditoría de cumplimiento para probar que cumple, una vez ha empezado a funcionar, los requisitos de seguridad y de operación necesarios para cumplir la política de los servicios de certificación del Consejo General del Notariado.

8.1.1. Frecuencia de la auditoría de conformidad

Se debe llevar a cabo una auditoría de conformidad anualmente, además de las auditorías internas que pueda llevar a cabo bajo su propio criterio o en cualquier momento, a causa de una sospecha de incumplimiento de alguna medida de seguridad o por un compromiso de claves.

8.1.2. Identificación y calificación del auditor

Si la Agencia Notarial de Certificación dispone de un departamento de auditoría interno, éste podrá encargarse de llevar a cabo la auditoría de conformidad.

En el caso de no poseer ese departamento, o de considerarlos oportuno, se deberá acudir a un auditor independiente, el cual debe demostrar experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública.

8.1.3. Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros deben ser llevadas a cabo por una entidad independiente de la Agencia Notarial de Certificación, no debiendo tener ningún conflicto de intereses que menoscabe su capacidad de llevar a cabo servicios de auditoría.

8.1.4. Listado de elementos objeto de auditoría

Los elementos objeto de auditoría serán los siguientes:

- Procesos de certificación de clave pública.
- Sistemas de información.
- Protección del centro de proceso
- Documentación del servicio.

Los detalles de cómo llevar a cabo la auditoría de cada uno de estos elementos se detallarán en el plan de auditoría de la Agencia Notarial de Certificación.

8.1.5. Acciones a emprender como resultado de una falta de conformidad

Una vez recibido el informe de la auditoría de cumplimiento llevada a cabo, la Agencia Notarial de Certificación debe discutir, con la entidad que ha ejecutado la auditoría y, en su caso, con el Consejo General del Notariado, las deficiencias encontradas y desarrollar y ejecutar un plan correctivo que solvente dichas deficiencias.

Si la Agencia Notarial de Certificación no es capaz de desarrollar y/o ejecutar el mencionado plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá realizarse una de las siguientes acciones:

- Revocar la clave de las Entidades de Certificación, tal y como se describe en la sección 5.7.2 de esta política.
- Terminar los servicios de certificación, tal y como se describe en la sección 5.8 de esta política.

8.1.6. Tratamiento de los informes de auditoría

La Agencia Notarial de Certificación debe entregar los informes de resultados de auditoría, al Consejo General del Notariado, en un plazo máximo de 15 días tras la ejecución de la auditoría.

9. Requisitos comerciales y legales

9.1. Tarifas

9.1.1. Tarifa de emisión o renovación de certificados

La Agencia Notarial de Certificación podrá establecer una tarifa por la emisión o por la renovación de los certificados, que deberá ser aprobada por el Consejo General del Notariado.

9.1.2. Tarifa de acceso a certificados

La Agencia Notarial de Certificación no podrá establecer ninguna tarifa por el acceso a los certificados.

9.1.3. Tarifa de acceso a información de estado de certificado

La Agencia Notarial de Certificación no podrá establecer ninguna tarifa por el acceso a la información de estado de los certificados.

9.1.4. Tarifas de otros servicios

Sin estipulación.

9.1.5. Política de reintegro

La Agencia Notarial de Certificación debe disponer de una política de reintegro de la tarifa, que deberá documentar en su Declaración de Prácticas de Certificación.

9.2. Capacidad financiera

La Agencia Notarial de Certificación deberá disponer de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios.

La Agencia Notarial de Certificación no se desempeña como agente fiduciario ni representante en forma alguna de los usuarios ni de los terceros de confianza en los certificados que emite.

9.2.1. Cobertura de seguro

La Agencia Notarial de Certificación deberá disponer de una garantía de cobertura de su responsabilidad civil suficiente, bien mediante un seguro de responsabilidad civil profesional por errores y omisiones, bien mediante una fianza o aval.

La cuantía garantizada deberá ser de 3.000.000 de euros o superior.

9.2.2. Otros activos

Sin estipulación.

9.2.3. Cobertura de seguro para suscriptores y terceros que confían en certificados

Sin estipulación.

9.3. Confidencialidad

9.3.1. Informaciones confidenciales

Las siguientes informaciones, como mínimo, serán mantenidas confidenciales por la Agencia Notarial de Certificación:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por la Agencia Notarial de Certificación.
- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Agencia Notarial de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como “Confidencial”.

9.3.2. Informaciones no confidenciales

La siguiente información será considerada no confidencial:

- Los certificados emitidos o en trámite de emisión.

- La vinculación del suscriptor a un certificado emitido por una Entidad de Certificación.
- El nombre y los apellidos del suscriptor del certificado o del poseedor de claves, según proceda, así como cualesquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico del suscriptor del certificado o del poseedor de claves, según proceda, o la dirección de correo electrónico que corresponda.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (CRLs), así como las restantes informaciones de estado de revocación.
- La información contenida en el Depósito.
- Toda otra información que no esté indicada en la sección anterior de esta política.

9.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4. Divulgación legal de información

La Agencia Notarial de Certificación divulgará la información confidencial en los casos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado serán divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

Se indicarán estas circunstancias en la política de intimidad prevista en la sección 9.4 de esta política.

9.3.5. Divulgación de información por petición de su titular

La Agencia Notarial de Certificación incluirá, en la política de intimidad prevista en la sección 9.4 de esta política, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, del poseedor de claves, directamente a los mismos o a terceros.

9.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

9.4. Protección de datos personales

Para la prestación del servicio, la Agencia Notarial de Certificación precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales. Tales informaciones serán recabadas directamente de los afectados, con su consentimiento explícito o en los casos es los que la ley permita recabar la información sin consentimiento del afectado.

Se recabarán los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

La Agencia Notarial de Certificación ha desarrollado una política de intimidad, de acuerdo con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y ha documentado en su Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al análisis de riesgos llevado a cabo según lo previsto en dicho Reglamento.

La Agencia Notarial de Certificación no divulgará ni cederá datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6 de esta política, y en la sección 5.8, en caso de terminación de la Entidad de Certificación.

La información confidencial de acuerdo con la normativa de protección de datos será protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en el Reglamento indicado.

9.5. Derechos de propiedad intelectual

9.5.1. Propiedad de los certificados e información de revocación

La Agencia Notarial de Certificación será la única entidad que gozará de los derechos de propiedad intelectual sobre los certificados que emita, debiendo conceder 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 usos autorizado y legítimos de acuerdo con esta política, según se define en la sección 1.4, y de acuerdo con las correspondientes condiciones generales de uso.

Las mismas reglas resultarán de aplicación al uso de información de revocación de certificados.

9.5.2. Propiedad de la política de certificado y Declaración de Prácticas de Certificación

El Consejo General del Notariado será la única entidad que gozará de los derechos de propiedad intelectual sobre las políticas de certificados.

La Agencia Notarial de Certificación será propietaria de las Declaraciones de Prácticas de Certificación.

9.5.3. Propiedad de la información relativa a nombres

El suscriptor y, en su caso, el poseedor de claves, conservará cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor será el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1 de esta política.

9.5.4. Propiedad de claves

Los pares de claves serán propiedad de los suscriptores de los certificados.

Cuando una clave se encuentre fraccionada en partes, todas las partes de la clave serán propiedad del propietario de la clave.

9.6. Obligaciones y responsabilidad civil

9.6.1. Modelo de obligaciones del prestador de servicios de certificación

La Agencia Notarial de Certificación debe garantizar, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados.

Será la única entidad responsable del cumplimiento de los procedimientos descritos en esta política.

La Agencia Notarial de Certificación debe prestar sus servicios de certificación conforme con su Declaración de Prácticas de Certificación vigente, en la que se detallarán sus funciones, procedimientos de operación y medidas de seguridad.

Antes de la emisión y entrega del certificado al suscriptor, se deberá informarle de los términos y condiciones relativos al uso del certificado, de su precio – cuando se establezca – y de sus limitaciones de uso.

Este requisito se podrá cumplir mediante un "Texto divulgativo de la política de certificado" aplicable, que podrá ser transmitido electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Se debe vincular a suscriptores, poseedores de claves y terceros que confían en certificados mediante condiciones generales de emisión y uso de certificados, que deberán estar en lenguaje escrito y comprensible, y debe tener los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.2, 9.2, 9.6.7, 9.6.8, 9.6.9 y 9.6.10 de la presente política de certificación.
- Indicación de la política aplicable, con indicación de sí los certificados se expiden al público y de la necesidad de empleo de dispositivo cualificado.

- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión del dispositivo cualificado de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Entidad de Certificación sin revocación de certificados válidos.
- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2 de esta política.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Agencia Notarial de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Agencia Notarial de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Entidad de Certificación de certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2. Garantías ofrecidas a suscriptores y terceros que confían en certificados

La Agencia Notarial de Certificación, en las condiciones generales de emisión y uso de certificados, establecerá y rechazará garantías, y limitaciones de responsabilidad aplicables.

La Agencia Notarial de Certificación, como mínimo, garantizará al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Agencia Notarial de Certificación y, en su caso, por la entidad de registro.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.

- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

La Agencia Notarial de Certificación, como mínimo, garantizará al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.
- En caso de certificados publicados en el Depósito, que el certificado ha sido emitido al suscriptor identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4 de la presente política de certificación.
- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, cuando emita un certificado de firma electrónica, garantizará al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I del Reglamento (UE) 910/2014.
- La responsabilidad de la Agencia Notarial de Certificación, con los límites legales que se establezcan.

9.6.3. Rechazo de otras garantías

La Agencia Notarial de Certificación podrá rechazar toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 9.6.2.

9.6.4. Limitación de responsabilidades

La Agencia Notarial de Certificación limitará su responsabilidad a la emisión y gestión de certificados y, en su caso, de pares de claves de suscriptores y dispositivos criptográficos (de firma y verificación de firma, así como de cifrado o descifrado) suministrados por la Agencia Notarial de Certificación.

La Agencia Notarial de Certificación podrá limitar su responsabilidad mediante la inclusión de límites de uso del certificado, y límites de valor de las transacciones para las que puede emplearse el certificado.

9.6.5. Cláusulas de indemnidad

9.6.5.1. Cláusula de indemnidad de suscriptor

La Agencia Notarial de Certificación podrá incluir, en las condiciones generales de emisión de certificados, una cláusula por la cual el suscriptor se compromete a mantener indemne a la

Agencia Notarial de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión medió dolo o negligencia con respecto a la Agencia Notarial de Certificación, la entidad de registro o cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.6.5.2. Cláusula de indemnidad de tercero que confía en el certificado

La Agencia Notarial de Certificación podrá incluir, en las condiciones generales de uso de certificados, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Agencia Notarial de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Incumplimiento de las obligaciones del tercero que confía en el certificado.
- Confianza temeraria en un certificado, a tenor de las circunstancias.
- Falta de comprobación del estado de un certificado, para determinar que no se encuentra suspendido o revocado.

9.6.6. Caso fortuito y fuerza mayor

La Agencia Notarial de Certificación incluirá cláusulas para limitar su responsabilidad en caso fortuito y en caso de fuerza mayor, en las condiciones generales de emisión y uso de certificados.

9.6.7. Ley aplicable

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso de certificados, que la ley aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la ley española.

9.6.8. Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso de certificados, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, se velará porque, al menos los requisitos contenidos en las secciones 9.6.1 (Obligaciones y responsabilidad), 0 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación de los servicios.
- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.6.9. Cláusula de jurisdicción competente

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso de certificados, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles.

La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.6.10. Resolución de conflictos

La Agencia Notarial de Certificación deberá establecer, en las condiciones generales de emisión y uso de certificados, los procedimientos de mediación y resolución de conflictos aplicables.

Las situaciones de discrepancia que se deriven de la utilización del empleo de los certificados emitidos, se resolverán aplicando los mismos criterios de competencia que en los casos de los documentos firmados manuscritamente.