Declaración de Prácticas de Certificación

Certificados Corporativos

Versión: 1.9

Vigencia: 18/09/2023

ancert
Agencia Notarial de Certificación

1. Información general

1.1. Control documental

Proyecto:	**Declaración de Prácticas de Certificación clase Certificados Corporativos**
Entidad de destino:	**Agencia Notarial de Certificación, S.L.U.**
Código de referencia:	
Versión:	**1.9**
Fecha de la edición:	
Archivo:	**DPC_PRIV_V2_20230918.docx**
Formato:	**Word 2007**

1.2. Control de versiones

Versión	Partes que cambian	Descripción del cambio	Fecha cambio	Fecha publicación
1.1	Original	Creación del documento	27/03/2010	
1.2		Revisión del documento	05/05/2010	
1.3	1.3.1	Incorporación de las huellas digitales de los certificados de las CA	02/06/2010	
1.4	Logo ANCERT	Nuevo logo ANCERT	30/11/2010	
1.5		Revisión aspectos legales y formato	21/12/2010	01/01/2011
1.6	Sección 4.9.6 Sección 1.1.2 Secciones 1, 2, 3 y 4	CRL con 60 días de información histórica Descripción más detallada de los usos. Incorporación de la clase certificados corporativos de servidor seguro.	30/01/2011	01/03/2011
1.7	Secciones 4.1, 6.3.1, 6.9.3, 6.9.6, 6.9.9, 7.7.5 y 11.2	Adecuación controles AICPA/CICA WebTrust Program for CA v 2	01/06/2012	01/10/2012
1.8	Sección 8.2	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
1.9	Sección 3.5	Actualización domicilio social	18/09/2023	18/09/2023

2. Índice

3. Introducción

Este documento contiene la Declaración de prácticas de certificación que regula la clase de certificados "Certificados Corporativos" emitidos por la Agencia Notarial de Certificación.

3.1. Presentación

3.1.1. Clase de certificados Corporativos

La "Clase Corporativos" de certificados agrupa los certificados expedidos por la Agencia Notarial de Certificación a corporaciones privadas, actuando éstas como Entidades de Registro de sus usuarios.

3.1.2. Certificados que se emiten

Dentro de la "Clase Corporativos", se emiten los siguientes certificados:

3.1.2.1. Certificados Corporativos Personales

Los Certificados Corporativos Personales son certificados reconocidos, en los términos del artículo 11 de la Ley 59/2003, de Firma Electrónica; es decir, son certificados electrónicos expedidos por la Agencia Notarial de Certificación cumpliendo los requisitos establecidos en dicha Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que prestan.

Existen dos modalidades de Certificados Corporativos Personales:

- Los **Certificados Corporativos Personales con dispositivo seguro** de creación de firma.
- Los **Certificados Corporativos Personales sin dispositivo seguro** de creación de firma.

Los Certificados Corporativos Personales con dispositivo seguro de creación de firma permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

- La creación de la firma electrónica reconocida, que es la firma electrónica avanzada basada en un certificado reconocido y que se genera mediante un dispositivo seguro de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.
- La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia. El certificado de autenticación también puede utilizarse para la creación de firma electrónica avanzada de documentos electrónicos conforme a las condiciones acordadas por las partes para relacionarse entre sí, o cuando la normativa administrativa aplicable lo admita expresamente.
- El cifrado y el descifrado de documentos electrónicos.

Los Certificados Corporativos Personales sin dispositivo seguro de creación de firma permiten:

- Tres funcionalidades, emitiéndose todas en un único Certificado:
    - La creación de la firma electrónica avanzada basada en un certificado reconocido.
    - La autenticación personal en sistemas electrónicos de información, en presencia física o a distancia.
    - El cifrado y el descifrado de documentos electrónicos.

3.1.2.2. Certificados Corporativos de Sistemas

Los Certificados Corporativos de Sistemas son certificados para el aseguramiento informático de las operaciones de sistemas de información. Dichos certificados no tienen la consideración de certificados reconocidos, de acuerdo con la Ley 59/2003, de Firma Electrónica.

Existen dos modalidades de Certificados Corporativos de Sistemas:

- **Certificado Corporativos de Servidor Seguro**, que se emiten a una corporación privada en calidad de titular del nombre de dominio de servidores SSL/TLS, para el establecimiento de comunicaciones seguras y autenticadas entre servidor y cliente SSL/TLS.
- **Certificados Corporativos de Aplicación Segura**, que se emiten a una corporación privada en calidad de titular de aplicaciones informáticas de funcionamiento automatizado o a otras entidades cuyas aplicaciones informáticas necesitan intercambiar información con la aplicación del titular y que precisan las funciones de autenticación, firma digital o cifrado/descifrado.

Todas las funcionalidades del Certificado Corporativo de Aplicación Segura se contienen en un único certificado.

3.2. Nombre del documento e identificación

Este documento es la "Declaración de prácticas de certificación de los Certificados de "Clase Corporativos" de la Agencia Notarial de Certificación" y se le ha asignado el siguiente OID: ANCERT.0.1.0.3

El OID de ANCERT ES: 1.3.6.1.4.1.18920.

La Agencia Notarial de Certificación ha asignado los siguientes identificadores de objeto (OID) a los certificados, para su identificación por las aplicaciones:

Certificado	Identificador
Certificados Corporativos Personales (con dispositivo seguro para firma)	ANCERT 2.1.1.2.1
Certificados Corporativos Personales (con	ANCERT 2.1.1.2.2

dispositivo seguro para autenticación)	
Certificados Corporativos Personales (con dispositivo seguro para cifrado)	ANCERT 2.1.1.2.3
Certificados Corporativos Personales (sin dispositivo seguro)	ANCERT 2.1.1.2.4
Certificados Corporativos de Aplicación Segura (sin dispositivo seguro)	ANCERT 2.2.1.1.2
Certificado Corporativo de Servidor Seguro (sin dispositivo seguro)	ANCERT.2.2.2.1.2

La Agencia Notarial de Certificación publica en su Depósito un documento con los OIDs correspondientes a las prácticas de certificación y a los certificados vigentes en cada momento.

3.3. Participantes en los servicios de certificación

Esta Declaración de Prácticas de Certificación regula la prestación de servicios de certificación al público en general, emitiendo certificados a personas físicas donde la Entidad de Registro es una entidad privada la cual identifica y verifica las circunstancias personales de los Solicitantes de los certificados y asegura que tienen a su juicio capacidad y legitimación suficientes, y acredita de que el consentimiento ha sido libremente prestado y de que esta comprobación se adecua a la legislación y a la voluntad debidamente informada de dichos solicitantes.

Los participantes en los servicios de certificación serán los siguientes:

3.3.1. Prestador de Servicios de Certificación

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

Para esta clase "Certificados Corporativos, la Agencia Notarial de Certificación dispone de las siguientes Entidades de Certificación:

3.3.1.1. ANCERT Certificados Redes Privadas V2

ANCERT Certificados Redes Privadas V2 es la entidad de Certificación Raíz, basada en un certificado raíz autofirmado, cuya huella digital basada en el algoritmo SHA-1 es:

A49D 9A8A 21B5 C3D8 D59B 1B1D 5653 03DB 5A2B 45E8

ANCERT Certificados Redes privadas expide certificados raíz para las siguientes Entidades de Certificación subordinadas:

- ANCERT Corporativos Personales V2
- ANCERT Corporativos de Sistemas V2

3.3.1.2. ANCERT Corporativos Personales V2

Esta Entidad de Certificación subordinada emita los certificados electrónicos denominados Certificados Corporativos Personales.

La huella digital de esta Entidad de Certificación subordinada basada en el algoritmo SHA-1 es:

55D4 F862 B735 F945 7C3F 6D36 B259 719F 8FFA D728

3.3.1.3. ANCERT Corporativos de Sistemas V2

Esta Entidad de Certificación subordinada emita los certificados electrónicos denominados Certificados Corporativos de Aplicación Segura.

La huella digital de esta Entidad de Certificación subordinada basada en el algoritmo SHA-1 es:

6B2A 3E14 B64E 2FE7 5DD3 0F60 7A21 AF6E E198 22A4

3.3.2. Entidades de registro

Las entidades de registro son las personas físicas o jurídicas que asisten a la Agencia Notarial 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.

Para la clase de certificados emitidos por las Autoridades de Certificación subordinadas "ANCERT Corporativos Personales V2" y "ANCERT Corporativos de Sistemas V2" actúa como Entidad de Registro la misma Organización privada que es a su vez el Subscriptor del certificado.

3.3.3. Entidades finales

Las entidades finales son 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.
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) Terceros que confían en certificados.

3.3.3.1. Solicitantes de certificados

Los certificados corporativos deben ser solicitados por una persona física en nombre de una organización.

- En los **certificados corporativos personales**, esta persona física sin ser el futuro suscriptor del certificado solicitado, es el poseedor de claves.

- En los **certificados corporativos de aplicación segura** esta persona física actúa como representante legal o voluntario de una organización.

- En los **certificados corporativos de servidor seguro** esta persona física actúa como representante legal o voluntario de una organización.

3.3.3.2. Suscriptores de certificados

Los suscriptores son las organizaciones titulares del certificado.

Para los certificados que se emiten, de clase "Certificados Corporativos", los subscriptores son las personas jurídicas identificadas en el certificado.

3.3.3.3. Poseedores de claves

Los poseedores de claves son las personas físicas que poseen de forma exclusiva las claves criptográficas, que no son suscriptores del certificado. 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 y apellidos.

Los Certificados Corporativos de Servidor Seguro no emplean poseedores de claves.

3.3.3.4. Los Certificados Corporativos de Aplicación Segura pueden emplear el concepto de poseedor de las claves cuando sean entregados a otras entidades cuyas aplicaciones necesitan con la única finalidad de interaccionar con una aplicación del titular. En estos casos, la entidad poseedora de las claves se encuentra debidamente identificada en el certificado mediante su razón social y CIF.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 esta Declaración de prácticas de certificación y en los documentos jurídicos correspondientes.

3.4. Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada certificado de los emitidos para la clase "Certificados Corporativos", y establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

3.4.1. Usos permitidos para los certificados

Los certificados de Clase Corporativos pueden emplearse para los usos descritos en la sección 3.1.2 de esta Declaración de Prácticas de Certificación.

En relación con el uso de los certificados, debe entenderse lo siguiente:

- **Autenticidad de origen**: Asegura que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona o entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica. El receptor de un mensaje firmado electrónicamente puede verificar esa firma empleando el certificado.
- **Autenticidad de servidor**: Asegura que la comunicación electrónica proviene del servidor del que dice provenir. El usuario puede verificar la autenticidad del servidor a través del certificado.
- **Aceptación de contenido por el emisor**[1]: Evita que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo. Para ello se utiliza la firma electrónica. El receptor de un mensaje firmado digitalmente puede verificar esa firma empleando el certificado. De esta forma puede demostrar la identidad del emisor del mensaje y la aceptación de su contenido, sin que éste pueda refutarlos falsamente.
- **Integridad**: Permite comprobar que un documento electrónico para el que se ha generado una firma electrónica no ha sido modificado por ningún agente externo. Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (funciones de *hash*), utilizadas en combinación con la firma electrónica. El procedimiento se centra en firmar electrónicamente un resumen único del documento electrónico con la clave privada del suscriptor de forma que cualquier alteración del documento revierte en una alteración de su resumen.
- **Confidencialidad**: Asegura que los datos que se transmiten no pueden ser leídos por terceras personas sin autorización, ya que los datos que se envían están cifrados.

[1] También llamado frecuentemente "no repudio" o "irrefutabilidad".

3.4.2. Límites y prohibiciones de uso de los certificados

3.4.2.1. Límites de uso

Todos los certificados deben emplearse para su función propia y finalidad establecida en la descripción del certificado de la sección 3.1.2 de esta Declaración de Prácticas de Certificación, sin que puedan emplearse en otras funciones y con otras finalidades.

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

Los certificados pueden contener límites adicionales uso en forma de atributos dentro del campo *Subject Directory Attributes*, tal y como se indica en la sección 5.1.4 de esta Declaración de Prácticas de Certificación, así como en las condiciones generales de uso de los certificados. Los terceros deben considerar estas limitaciones antes de confiar en los certificados.

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.

A continuación se describen las informaciones adicionales que se encuentran contenidas en los certificados y que suponen o pueden suponer limitaciones en el uso de los certificados.

Los terceros deben considerar estas limitaciones antes de confiar en los certificados.

3.4.2.1.1. Indicación de límite de uso por razón de la cuantía

Los Certificados Corporativos Personales emitidos por la Autoridad de Certificación "ANCERT Corporativos Personales V2" se conceden sin limitación de uso por razón de la cuantía.

3.4.2.2. Prohibiciones de usos

Los Certificados Corporativos 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.

3.5. Administración del documento

3.5.1. Organización que administra el documento

Agencia Notarial de Certificación, S.L. Unipersonal

c/ Campezo, nº 1, Edificio 6, pl. 2ª, de (28022) Madrid (España)

NIF nº B-83395988

3.5.2. Datos de contacto de la organización

Cualquier contacto con la Agencia Notarial de Certificación, referente a esta Declaración de Prácticas de Certificación puede realizarse por los siguientes medios:

- Vía e-mail a la dirección de correo electrónico ancert@ancert.com.
- Por teléfono al número 902 348 347.
- Directamente en la sede central de la Agencia Notarial de Certificación: Agencia Notarial de Certificación, S.L. Unipersonal c/ Campezo, nº 1, Edificio 6, pl. 2ª, de (28022) Madrid (España)

Las alteraciones que se produzcan sobre los anteriores datos como Web, correo, dirección o teléfono constarán debidamente reflejadas en la página web www.ancert.com que la Agencia Notarial de Certificación mantiene en vigor en Internet.

3.5.3. Procedimientos de gestión del documento

Quien determina la idoneidad de esta Declaración de Prácticas de Certificación, y se encarga de su aprobación es el Consejo de Administración de la Agencia Notarial de Certificación.

La presente Declaración de Prácticas de Certificación de la clase de Certificados Corporativos puede ser modificada en cualquier momento por la Agencia Notarial de Certificación. De no aceptar cualquiera de los suscriptores con certificado en vigor alguna de las modificaciones acordadas puede instar la revocación de su Certificado.

La revocación así solicitada no da derecho a reclamar indemnización alguna, ni aun la devolución parcial del precio del certificado, salvo que la rectificación o modificación de esta Declaración de Prácticas de Certificación implique una limitación de los derechos de uso o una restricción sobre el ámbito de aplicación sobre el certificado emitido, en cuyo caso se podrá exigir el reembolso del precio del mismo.

4. Publicación de información y depósito de certificados

4.1. Depósito(s) de certificados

La Agencia Notarial de Certificación dispone de un Depósito de certificados. Los certificados se conservarán en el depósito hasta al menos un año después de su expiración.

El servicio de Depósito está disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Agencia Notarial de Certificación, ésta realiza sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 7.7.5 de esta Declaración de Prácticas de Certificación.

4.2. Publicación de información del prestador de servicios de certificación

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

- Los certificados emitidos, incluidos los certificados de Entidades de Certificación que emiten certificados para esta clase de certificados.
- 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 dicha política.
- Las diversas versiones de la Declaración de Prácticas de Certificación.
- Los documentos de condiciones generales vinculantes con suscriptores y terceros que confían en certificados.

4.3. Frecuencia de publicación

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

Los cambios en los documentos de política específica y en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 3.5 del documento de política o Declaración de Prácticas de Certificación.

La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 6.9.6 y 6.9.7 de esta Declaración de Prácticas de Certificación.

4.4. Control de acceso

La Agencia Notarial de Certificación no limita el acceso de lectura a las informaciones establecidas en la sección 4.2, pero establece 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.

La Agencia Notarial de Certificación emplea 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.

5. Identificación y autenticación

5.1. Gestión de nombres

5.1.1. Tipos de nombres

Todos los certificados contienen un nombre diferenciado de la persona y/o organización, identificados en el certificado, definido de acuerdo con lo previsto en la Recomendación ITU-T X.501 y contenido en el campo *Subject Name*.

Los certificados contienen nombres alternativos de las personas y organizaciones identificadas en los certificados, principalmente en el campo *SubjectAlternativeName*.

Las circunstancias personales y atributos de las personas y organizaciones identificadas en los certificados se incluyen en atributos predefinidos en normas y especificaciones técnicas ampliamente utilizadas en el sector o sectores de actividad donde deban emplearse los certificados, así como en atributos definidos de forma específica por la Agencia Notarial de Certificación, principalmente en el campo *Subject Directory Attributes*

5.1.2. Significado de los nombres

Los nombres de los certificados son 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 son tratados de acuerdo con las siguientes normas:

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

5.1.3. Empleo de anónimos y seudónimos

En esta clase de certificados no se emiten certificados anónimos ni certificados de seudónimo.

5.1.4. Interpretación de formatos de nombres

La Agencia Notarial de Certificación emplea los siguientes esquemas de nombres:

Certificado Corporativo Personal con dispositivo seguro:

SUBJECT NAME	
CAMPO	**CONTENIDO**
Country (C)	País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)
Organization (O)	Nombre de la entidad suscriptora.
Organizational Unit(OU)	Campo libre (sólo para indicar una división departamental de la entidad.
Organizational Unit(OU)	"Certificado Corporativo Personal (" + "Firma" o "Autentica" o "Cifrado" + ")"
Title	Rol o función del poseedor de claves.
Surname (SU)	Apellidos del poseedor de claves.
Given Name (GN)	Nombre del poseedor de claves.
Serial Number	NIF del poseedor de claves (NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas)
Common Name (CN)	Nombre y apellidos del poseedor de claves.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Correo electrónico.
SUBJECT DIRECTORY ATTRIBUTES	
ANCERT.10.1.1	“Sin garantía de poderes”
ANCERT.10.1.4	Atributos adicionales del poseedor de claves.

Certificado Corporativo Personal sin dispositivo seguro:

SUBJECT NAME	
CAMPO	**CONTENIDO**
Country (C)	País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)
Organization (O)	Nombre de la entidad suscriptora.
Organizational Unit(OU)	Campo libre (sólo para indicar una división departamental de la entidad.
Organizational Unit(OU)	"Certificado Corporativo Personal”
Title	Rol o función del poseedor de claves.
Surname (SU)	Apellidos del poseedor de claves.

Given Name (GN)	Nombre del poseedor de claves.
Serial Number	NIF del poseedor de claves (NIF de la persona física identificada, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas)
Common Name (CN)	Nombre y apellidos del poseedor de claves.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Correo electrónico.
SUBJECT DIRECTORY ATTRIBUTES	
ANCERT.10.1.1	"Sin garantía de poderes"
ANCERT.10.1.4	Atributos adicionales del poseedor de claves.

Certificado Corporativo de Aplicación Segura:

SUBJECT NAME	
CAMPO	**CONTENIDO**
Country (C)	País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)
Organization (O)	Nombre de la entidad poseedora de las claves.
Organizational Unit(OU)	"Certificado Corporativo de Aplicación Segura"
Serial Number	CIF de la entidad poseedora de las claves.
Common Name (CN)	Identificador de la aplicación segura del suscriptor.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Correo electrónico.

Certificado Corporativo de Servidor Seguro:

SUBJECT NAME	
CAMPO	**CONTENIDO**
Country (C)	País (nacionalidad de la persona física identificada, indicándose el código de dos letras especificado en la norma ISO 3166)
Organization (O)	Nombre de la entidad suscriptora.
Organizational Unit(OU)	"Certificado Corporativo de Servidor Seguro"
Serial Number	CIF de la entidad suscriptora.
Common Name (CN)	Nombre del servidor y dominio.
SUBJECT ALTERNATIVE NAME	
rfc822Name	Correo electrónico.

dnsName	Otros nombres del servidor y dominios.

5.1.4.1. Indicación de límites de uso

5.1.4.1.1. Indicación de la clase de apoderamiento

- Este límite de uso se contiene en el atributo ANCERT.10.1.1, dentro del campo *Subject Directory Attributes* de los Certificados Corporativos

El límite de uso corresponde al nivel de garantía en relación con el apoderamiento, indicando también la ausencia de garantía con respecto a los poderes de una persona física, con las siguientes posibilidades:

- "Sin garantía de poderes", que se emplea para indicar que el certificado se emite sin haber comprobado si la persona tiene algún poder de actuación.

5.1.4.2. Indicación de atributos adicionales de la persona física

Los Certificados Corporativos pueden incorporar atributos adicionales de la persona física solicitante, como por ejemplo: pertenencia a una Organización, cargos honoríficos, etc…), dentro del atributo ANCERT.10.1.4 del campo *Subject Directory Attributes*.

5.1.4.3. Publicación en el Depósito

La Agencia Notarial de Certificación publica 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.

5.1.5. Unicidad de los nombres

Los nombres de los suscriptores de certificados son únicos para cada Entidad de Certificación operada por la Agencia Notarial de Certificación. Una persona sólo puede 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 asigna un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente.

5.1.6. Resolución de conflictos relativos a nombres

Los conflictos de nombres 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.

5.2. Validación inicial de la identidad

En esta sección se declaran 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.

5.2.1. 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 seguro 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 seguro y del correspondiente certificado y par de claves almacenados en su interior.

5.2.2. Autenticación de la identidad de una persona física

El proceso de identificación y autenticación de una persona física se realiza exclusivamente mediante la personación ante la Organización a la que está vinculada, que actúa como entidad de registro.

5.2.2.1. Elementos de identificación requeridos

- Los tipos de documentos que son necesarios para acreditar la identidad de una persona física son exclusivamente el documento nacional de identidad, la tarjeta de residencia, el

pasaporte, o cualquier otro medio admitido en derecho, siempre que contenga al menos la siguiente información: Nombre y apellidos

- Fecha de nacimiento
- Número de identidad reconocido legalmente

5.2.2.2. Validación de los elementos de identificación

La validación de los elementos de identificación requeridos lo realiza exclusivamente el legal representante de la Organización o Entidad privada, que actúa como Entidad de Registro de la Agencia Notarial de Certificación.

5.2.2.3. Necesidad de presencia personal

Para los certificados corporativos es necesaria la presencia de la persona identificada en el certificado.

Se puede obviar esta presencia cuando:

- la Organización hubiera identificado con anterioridad a la persona física, y el período de tiempo transcurrido desde esta identificación sea menor de cinco años,
- cuando en el momento de solicitar un certificado se utilice otro vigente, cuya expedición se hubiera identificado al poseedor de claves con su presencia ante la Entidad de Registro.

5.2.2.4. Vinculación de la persona física con la Organización

En los certificados corporativos la persona física o poseedor de claves tiene una vinculación con la Organización (suscriptor del certificado).

El legal representante de la Organización debe cerciorarse que la vinculación de la persona física con la Organización aún existe, realizando las comprobaciones necesarias con su responsable de personal o con el departamento correspondiente encargado de los contratos de personal, altas y bajas, o similares.

5.2.3. Información de suscriptor no verificada

No se incluye información de suscriptor no verificada en los certificados.

5.3. Identificación y autenticación de solicitudes de renovación con cambio de claves

5.3.1. Validación para la renovación rutinaria de certificados

Se pueden renovar los Certificados Corporativos, siempre que sea durante su período de vigencia o en un plazo máximo de tres meses después de su expiración.

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

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

Si cualquier información del suscriptor o del poseedor de la clave ha cambiado, se registra adecuadamente la nueva información, de acuerdo con lo establecido en la sección 5.2.

5.3.2. Validación para la renovación de certificados tras la revocación

No resulta aplicable, debido a que la Agencia Notarial de Certificación no renueva en ningún caso certificados que han sido revocados.

5.4. Identificación y autenticación de la solicitud de suspensión

El legítimo solicitante debe telefonear al número 902 348 347 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación.

5.5. Identificación y autenticación de la solicitud de revocación

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

Esta solicitud de revocación de los Certificados Corporativos personales se realiza:

- A instancia de la Entidad de Registro. Ésta puede solicitar la suspensión de los certificados emitidos.
- A instancia de la AGENCIA NOTARIAL DE CERTIFICACIÓN la cual podrá proceder a la revocación del Certificado cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en este documento.

En todos los casos, una vez revocado el Certificado, la revocación será publicada en el Directorio de Certificados de la AGENCIA NOTARIAL DE CERTIFICACIÓN, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la Lista de Certificados Revocados en el plazo máximo previsto de veinticuatro (24) horas.

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

6.1. Solicitud de emisión de certificado

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

Existen 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 registro, 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 5.2.1 de la presente Declaración de Prácticas de Certificación).

6.1.1. Legitimación para solicitar la emisión

Están legitimados para solicitar la emisión de un certificado:

- La persona que indique la Organización y esté autorizada por dicha Organización.

6.1.2. Procedimiento de alta; Responsabilidades

La fase de solicitud del certificado comprende con carácter general la personación ante la Entidad de Registro, para la comprobación y confirmación de la identidad personal del solicitante.

La Organización como Entidad de Registro de la Agencia Notarial de Certificación asegura que las solicitudes de certificado son completas, precisas y están debidamente autorizadas.

Antes de la emisión y entrega del certificado, la entidad de registro informa al poseedor de claves de los términos y condiciones aplicables al certificado.

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

A la solicitud se acompaña 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 **¡Error! No se encuentra el origen de la referencia.** y 5.2.2 de esta Declaración de prácticas de Certificación.

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

En los certificados Corporativos Personales la correspondiente Entidad de Registro se encuentra obligada al cumplimento de las mismas obligaciones y en iguales condiciones que la Agencia Notarial de Certificación.

6.2. Procesamiento de la solicitud de certificación

6.2.1. Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, la entidad de registro verifica la información proporcionada, conforme a la sección 5.2 de esta Declaración de Prácticas de Certificación, mediante el siguiente procedimiento:

- Se realiza un expediente en papel o con tramitación electrónica
- El poseedor de claves se persona físicamente en la Entidad de Registro
- Se le identifica con el original de su documento que lo identifica (ver apartado 5.2.2).

6.2.2. Aprobación o rechazo de la solicitud

Si la verificación no es correcta, o si se sospecha que no es correcta, la entidad de registro deniega la petición, o detiene su aprobación hasta realizar las comprobaciones oportunas.

En caso de que los datos se verifiquen correctamente, la entidad de registro aprueba la solicitud del certificado, aprobación que notifica al solicitante.

Asimismo, se solicita a la Entidad de Certificación ANCERT Certificados Corporativos la generación del certificado.

Si hay una incidencia por la que el procedimiento no se lleva a cabo se rellena un formulario que se envía a la entidad de certificación.

6.2.3. Plazo para resolver la solicitud

Sin estipulación.

6.3. Emisión del certificado

6.3.1. Acciones durante el proceso de emisión

Para la emisión de un certificado el operador, actuando como entidad de registro, debe acceder a la aplicación de emisión de certificados. El acceso a la aplicación está protegido, identificando al operador mediante su certificado digital. La aplicación comprueba que el operador, una vez autenticado, está autorizado para emitir el certificado. De esta forma se asegura que la comunicación entre la RA y la CA se lleva a cabo de forma segura.

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado. Las acciones a seguir para la emisión de las claves y el certificado son distintas, según si el soporte para su almacenamiento es una tarjeta criptográfica o en software.

En todos los casos, la Agencia Notarial de Certificación:

- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.

- Protege la confidencialidad e integridad de los datos de registro, especialmente en caso de que sean intercambiados electrónicamente con el solicitante, durante la presolicitud.
- Incluye en el certificado las informaciones establecidas en el artículo 11 de la Ley 59/2003, de 19 de diciembre, de acuerdo con lo establecido en las secciones 5.1 y 9.1 de esta Declaración de Prácticas de Certificación.
- Indica la fecha y la hora en que se expide el certificado.
- En los casos en que la Agencia Notarial de Certificación aporta el dispositivo seguro de creación de firma se emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegura que dicho dispositivo es entregado de forma segura al poseedor de claves.
- Utiliza sistemas y productos fiables que están protegidos contra toda alteración y que garantizan la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Asegura que el certificado es emitido por sistemas que utilizan protección contra falsificación y, cuando genera claves privadas, que garantizan la confidencialidad de las claves durante el proceso de generación de dichas claves.

6.3.1.1. Emisión en tarjeta criptográfica

Para los Certificados Corporativos Personales en los que el soporte es una tarjeta criptográfica, las acciones a seguir son las siguientes:

1. El legal representante de la Organización asignado por ésta para esta tarea introduce en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como entidad de registro y accede a la aplicación de registro.

2. Una vez autenticado, introduce en el lector de tarjetas la tarjeta criptográfica del poseedor de claves. ANCERT Certificados Corporativos previamente a este momento ha facilitado a la Entidad de Registro las tarjetas solicitadas, en blanco, así como los códigos PIN y PUK correspondientes, en sobre cerrado.

3. El legal representante de la Organización completa el formulario de registro con los datos que le debe aportar el solicitante y solicita la emisión del certificado.

4. En este momento, la aplicación de registro solicita el PIN correspondiente a la tarjeta criptográfica del solicitante, para activar el procedimiento de generación de claves.

5. En ese momento se genera el par de claves en la tarjeta criptográfica del suscriptor, enviando la petición a la Agencia Notarial de Certificación, la cual genera el certificado y lo remite al ordenador de la Entidad de Registro vía SSL, quedando almacenado automáticamente en la tarjeta criptográfica del suscriptor.

6. El sistema genera automáticamente una factura, por el importe que consta en la web de la Agencia Notarial de Certificación www.ancert.com.

6.3.1.2. Emisión en software

Para los Certificados emitidos en software se utilizan como soporte los sistemas operativos o aplicaciones informáticas de los usuarios finales.

Las acciones a seguir para la emisión en software de los certificados corporativos personales son las siguientes:

1. El solicitante debe presentar a la Entidad de Registro el archivo en formato PKCS10 que contiene la petición de certificado.

2. El legal representante de la Entidad de Registro procede a introducir en el lector de tarjetas su tarjeta criptográfica con el certificado que le autentica como autorizado de la Entidad de Registro para emitir Certificados Corporativos Personales y accede a la aplicación de registro.

3. Este autorizado de la Entidad de Registro comprueba, mediante las herramientas que le proporciona la Agencia Notarial de Certificación, que el archivo facilitado por el solicitante corresponde con la información aportada y el perfil del certificado.

4. Si los datos son correctos completa el formulario de petición de certificado y envía la petición a la Agencia Notarial de Certificación.

5. En un plazo máximo de 48 horas, el solicitante puede obtener su Certificado Corporativo descargándolo de la dirección www.ancert.com.

6. El sistema genera automáticamente una factura, por el importe que consta en la web de la Agencia Notarial de Certificación www.ancert.com.

Para la emisión de los certificados corporativos de aplicación el proceso de emisión es el mismo que para los certificados corporativos personales en software.

6.3.2. Notificación de la emisión al suscriptor

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

En certificados emitidos a claves generadas en dispositivos seguros que estuvieran previamente en poder del solicitante, se notifica que el certificado se encuentra disponible en un plazo máximo de 48 horas, y que el solicitante puede obtener su Certificado Corporativo descargándolo de la dirección www.ancert.com.

6.4. Entrega y aceptación del certificado

6.4.1. Responsabilidades de la Agencia Notarial de Certificación

La Agencia Notarial de Certificación:

- Proporciona al suscriptor o al poseedor de claves, acceso al certificado, entregando, en su caso, el dispositivo seguro.
- Entrega al solicitante o al poseedor de claves una hoja de entrega del certificado y unas condiciones generales de emisión del certificado, 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, cuando existiera, del dispositivo seguro.

  c) Reconocimiento por parte de suscriptor o poseedor de claves, según proceda, de recibir el certificado y, en su caso, el dispositivo seguro, 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 seguro, de acuerdo con lo establecido en las secciones 8.2 y 8.4 de esta Declaración de Prácticas de Certificación.

  g) La fecha del acto de entrega y aceptación.

6.4.2. Conducta que constituye aceptación del certificado

La aceptación de los Certificados por parte del Suscriptor se entiende producida desde el momento de su emisión y entrega al mismo por la Agencia Notarial de Certificación y firma de la correspondiente hoja de entrega.

Al aceptar el Certificado el Suscriptor también acepta además las normas de uso y las condiciones contenidas en la presente Declaración de Prácticas de Certificación.

En todo caso, al aceptar un Certificado emitido por la Agencia Notarial de Certificación, el Suscriptor del mismo declara:

- Que toda la información entregada durante el procedimiento de solicitud del Certificado es verdadera.
- Que el Certificado será usado exclusivamente para fines legales y autorizados por la Agencia Notarial de Certificación de acuerdo a la presente Declaración de Prácticas de Certificación y siempre dentro del ámbito determinado en la Política de Certificación.
- Que asegura su exclusivo control sobre los Datos de creación de Firma que se correspondan con los Datos de verificación de Firma incluidos en su Certificado emitido por Agencia Notarial de Certificación y vinculados a su identidad personal, lo que, en todo caso y a título

meramente enunciativo, incluirá las acciones y medidas necesarias para prevenir su pérdida, revelación, modificación, o uso por tercero distinto del Suscriptor.

La Agencia Notarial de Certificación considerará válido todo Certificado aceptado por el Suscriptor y publicado en su Directorio de Certificados correspondiente, siempre que no haya caducado y que no conozca ninguna causa de revocación que le afecte.

6.4.3. Publicación del certificado

Una vez emitido el certificado, la Agencia Notarial de Certificación publica automáticamente una copia del mismo en el Depósito a que se refiere la sección 4.1 de esta Declaración de Prácticas de Certificación, con los controles de acceso pertinentes.

6.4.4. Notificación de la emisión a terceros

La Agencia Notarial de Certificación no notifica la emisión de certificados a terceros.

6.5. Uso del par de claves y del certificado

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

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

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

- En caso que el suscriptor genere sus propias claves, a:

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

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

  c) Emplear longitudes y algoritmos de clave reconocidos como aceptables para la firma electrónica reconocida.
- Facilitar a la Agencia Notarial de Certificación y a sus entidades de registro información completa y adecuada, 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 Declaración de Prácticas de Certificación.
- Emplear el certificado de acuerdo con lo establecido en la sección 3.4 de esta Declaración de Prácticas de Certificación.

- 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 8.1, 8.2 y 8.4 de esta Declaración de Prácticas de Certificación, 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 seguro.

  b) La pérdida de control sobre su clave privada o del dispositivo seguro, debido al compromiso de los datos de activación (por ejemplo, el código PIN del dispositivo seguro 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 8.3.2 de esta Declaración de Prácticas de Certificación.
- 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 reconoce, en el debido documento jurídico, que tales firmas electrónicas son firmas electrónicas equivalentes a firmas manuscritas, conforme a lo establecido en el artículo 3 de la Ley 59/2003, de 19 de diciembre.

6.5.1.2. Responsabilidad civil del suscriptor de certificado

La Agencia Notarial de Certificación obliga 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 esta Declaración de Prácticas de Certificación.

- 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.
- Que el suscriptor es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada y, en su caso, de generar correctamente dicha clave y emplear un dispositivo seguro de firma.

6.5.2. Uso por el tercero que confía en certificados

6.5.2.1. Obligaciones del tercero que confía en certificados

La Agencia Notarial de Certificación obliga 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.
- En relación con los certificados que permiten la firma electrónica, reconocer que las firmas electrónicas válidamente verificadas con los certificados son firmas electrónicas

equivalentes a firmas manuscritas, de acuerdo con el artículo 3 de la Ley 59/2003, de 19 de diciembre.

6.5.2.2. Responsabilidad civil del tercero que confía en certificados

La Agencia Notarial de Certificación obliga 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.

6.6. Renovación de certificados

Los certificados vigentes se pueden 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 puede realizar con o sin la renovación de las claves, en este caso de acuerdo con lo establecido en la sección 6.7 de este documento.

Los certificados pueden ser renovados durante su periodo de vigencia o en un plazo máximo de tres meses después de su expiración.

6.7. Renovación de claves y certificados

6.7.1. Causas de renovación de claves y certificados

Los certificados deben renovarse conjuntamente con las claves cuando se llegue al final del periodo de vida de las mismas, o del periodo de vida del dispositivo seguro en que se contengan.

6.7.2. Legitimación para solicitar la renovación

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

6.7.3. Procesamiento de la solicitud de renovación

La solicitud de renovación es realizada y enviada por el suscriptor o el poseedor de claves, con su certificado vigente, como prueba de posesión de clave privada, siempre que no hayan transcurrido más de cinco años desde la emisión del certificado a renovar.

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

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

6.7.4. Notificación de la emisión del certificado renovado

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

6.7.5. Conducta que constituye aceptación del certificado

Sin estipulación.

6.7.6. Publicación del certificado

La Agencia Notarial de Certificación publica el certificado renovado en el Depósito a que se refiere la sección 4.1, con los controles de seguridad pertinentes.

6.7.7. Notificación de la emisión a terceros

La Agencia Notarial de Certificación no notifica la renovación de certificados a terceros.

6.8. Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada, que se considera renovación, se trata como una nueva emisión de certificado, aplicándose lo descrito en las secciones 6.1 a 6.4 de esta Declaración de Prácticas de Certificación.

6.9. Revocación y suspensión de certificados

6.9.1. Causas de revocación de certificados

La Agencia Notarial de Certificación revoca 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 de la Entidad de Certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por la Agencia Notarial de Certificación, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas 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 la Agencia Notarial de Certificación y el suscriptor.

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 esta Declaración de Prácticas de Certificación.

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 5.5 de esta Declaración de Prácticas de Certificación.

5) Otras circunstancias:

a) La suspensión del certificado digital por un período superior al establecido en la sección 6.9.14 de esta Declaración de Prácticas de Certificación.

b) La terminación del servicio por la Agencia Notarial de Certificación, de acuerdo con lo establecido en la sección 7.8 de esta Declaración de Prácticas de Certificación.

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

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

6.9.2. Legitimación para solicitar la revocación

Están legitimados para solicitar la revocación de un certificado:

- En todo caso el suscriptor a nombre del cual el certificado fue emitido. La Organización, como suscriptor del certificado, debe actuar a través de una persona física con facultades jurídicas suficientes para revocar el certificado.

6.9.3. 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, 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 puede hacer una llamada, solicitando la suspensión, o enviar un correo electrónico a la Agencia Notarial de Certificación a la dirección electrónica *revocacion@ancert.com*.

La solicitud es autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 5.5 de esta Declaración de Prácticas de Certificación, antes de proceder a la revocación.

En caso de que el destinatario de la solicitud sea una entidad de registro, esta deberá:

- Identificar al solicitante de acuerdo con los requisitos establecidos en la sección 5.5 de esta Declaración de Prácticas de Certificación.
- Verificar que el solicitante está autorizado a solicitar la revocación del certificado.
- Solicitar la revocación accediendo a la aplicación telemática de revocación.

La solicitud de revocación es procesada a su recepción.

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

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

6.9.4. 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.

6.9.5. 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 suministra información a los terceros que confían en certificados acerca de cómo y dónde encontrar la Lista de Revocación de Certificados correspondiente; entre otros métodos, mediante la inclusión de la dirección web de publicación de las listas dentro de los propios certificados emitidos.

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

La Agencia Notarial de Certificación emite una nueva CRL al menos cada 24 horas. Adicionalmente, se emitirá una nueva CRL en un periodo de tiempo no superior a 15 minutos después de la suspensión o revocación de un certificado.

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

Los certificados revocados que expiran son retirados de la CRL transcurridos sesenta días desde su expiración.

6.9.7. Disponibilidad de servicios de comprobación de estado de certificados

De forma alternativa, los terceros que confían en certificados pueden consultar su estado en el Depósito de certificados de la Agencia Notarial de Certificación, que se encuentra disponible las 24 horas de los 7 días de la semana, en la dirección web *http://www.ancert.com.*

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 realizará sus mejores esfuerzos para asegurar que este servicio se mantiene inactivo el mínimo tiempo posible.

6.9.8. 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, debe emplear el Depósito para ello.

6.9.9. Otras formas de información de revocación de certificados

La Agencia Notarial de Certificación dispone de un servicio OCSP público para suministrar información de estado sobre los certificados, accesible en la dirección web indicada en los propios certificados emitidos.

La petición OCSP para la consulta del estado de un certificado debe incluir el número de serie del certificado y los datos identificativos de la autoridad de certificación emisora del mismo.

La respuesta generada por el servicio OCSP contiene la información de estado del certificado en el momento de la consulta. Si la petición no se puede satisfacer, el servidor generará una respuesta de error. Las respuestas OCSP son firmadas con la clave privada correspondiente a un Certificado Notarial de OCSP Trusted Responder.

6.9.10. 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.

Dicha notificación se produce, al menos, mediante la publicación de la información en el Depósito de la Agencia Notarial de Certificación.

6.9.11. Causas de suspensión de certificados

La Agencia Notarial de Certificación puede 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.

6.9.12. Legitimación para solicitar la suspensión

Pueden solicitar la suspensión de un certificado el suscriptor, la persona física o un tercero autorizado.

También puede solicitar la suspensión la Agencia Notarial de Certificación, cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de suspensión

6.9.13. Procedimientos de petición de suspensión

Para proceder a una solicitud electrónica de suspensión, el suscriptor o, en su caso el poseedor de claves, debe telefonear al teléfono 902 348 347 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante de la suspensión podrá ser sometida a grabación y almacenada en un dispositivo seguro.

En ningún caso cabe solicitar la suspensión de un certificado mediante envío de correo electrónico.

6.9.14. Plazo máximo de suspensión

El plazo máximo de suspensión es de sesenta (60) días naturales desde la fecha en que la Agencia Notarial de Certificación tenga conocimiento efectivo de cualquiera de las causas de suspensión, y así lo haga constar en el Depósito de Certificados y en la Lista de Revocación de Certificados.

6.9.15. Levantamiento de la suspensión

Los suscriptores podrán solicitar el levantamiento de la suspensión durante los sesenta (60) días siguientes a su suspensión debiendo telefonear al teléfono 902 348 347 del Centro de Atención a Usuarios de la Agencia Notarial de Certificación. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante será sometida a grabación.

El solicitante del levantamiento de la suspensión deberá responder con la contraseña que hubiera hecho constar a estos efectos en el proceso de solicitud del certificado. En caso de que la respuesta coincida con dicha contraseña el operador procederá a levantar la suspensión del certificado.

En todos los casos, una vez levantada la suspensión del Certificado, la misma será publicada en el acto en el Depósito de Certificados de la Agencia Notarial de Certificación, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la Lista de Certificados Revocados (CRL) en el plazo máximo previsto de veinticuatro (24) horas.

En el caso de que la suspensión haya provenido de la Agencia Notarial de Certificación éste únicamente podrá proceder a levantar la suspensión del certificado cuando por medio fehaciente haya tenido conocimiento cierto de la desaparición de la causa que motivó la suspensión. En este caso, inmediatamente después procederá a eliminar el Certificado de la Lista de Revocación.

6.9.16. Notificación de la revocación o suspensión

El suscriptor cuyo certificado haya sido suspendido o revocado debe ser informado de dicho hecho, así como, en su caso, del levantamiento de la suspensión, por lo que la Agencia Notarial de Certificación notificará dicha información por correo electrónico o postal o incluso por teléfono cuando no haya sido posible la notificación en alguna de las dos formas anteriores.

No obstante lo dispuesto en el párrafo anterior, la notificación se entenderá debidamente cumplimentada cuando haya sido realizada por correo electrónico a la dirección que aparezca en el certificado y que, por tanto, habrá sido admitida previamente por el usuario del certificado.

No obstante, si el sistema produjera un mensaje de error o rechazara la comunicación, se entenderá que la Agencia Notarial de Certificación ha cumplido suficientemente la notificación cuando ésta haya sido sellada. A fin de justificar ulteriormente el cumplimiento de la debida diligencia, la Agencia Notarial de Certificación conservará durante quince años el comprobante electrónico de haber realizado la comunicación de la revocación o suspensión.

La extinción o suspensión de la vigencia de un certificado electrónico se mantendrá accesible en el directorio de Listas de Revocación de Certificados al menos hasta la fecha en que hubiera finalizado su período inicial de validez.

6.10. Servicios de comprobación de estado de certificados

6.10.1. Características operativas de los servicios

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

6.10.2. Disponibilidad de los servicios

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

6.10.3. Características opcionales

Sin estipulación.

6.11. Finalización de la suscripción

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

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

6.12. Depósito y recuperación de claves

6.12.1. Política y prácticas de depósito y recuperación de claves

La Agencia Notarial de Certificación no deposita ni puede recuperar claves de suscriptores o poseedores de claves, con excepción de las claves de los certificados de cifrado, que se encuentran depositadas en la Agencia Notarial de Certificación, con controles de seguridad apropiados que impiden su acceso no autorizado por terceras personas.

Las claves de cifrado sólo se pueden recuperar a solicitud de la persona física identificada en el certificado, y en caso de mandamiento judicial, mediante el correspondiente procedimiento implantado por la Agencia Notarial de Certificación.

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

Sin estipulación.

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

Diferenciamos en este apartado diversos dominios de actuación en la Agencia Notarial de Certificación, que son:

- Dominio de creación de certificados.

  Los controles de seguridad física, de gestión y de operaciones en el dominio de creación de los certificados son operados directamente por la Agencia Notarial de Certificación y se realizan de acuerdo con su política de certificación y esta declaración de prácticas de certificación.

- Dominio de registro de usuario y gestión de tarjetas en la Organización.

  Los controles de seguridad física, de gestión y de operaciones en el dominio de registro y la gestión de tarjetas criptográficas son operados por un representante legal de la Organización.

7.1. Controles de seguridad física

Dominio de creación de certificados

La Agencia Notarial de Certificación disponer de instalaciones que protegen 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 logra 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 se encuentra fuera de estos perímetros.

La Agencia Notarial de Certificación ha establecido 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 establece prescripciones para las siguientes contingencias:

- 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.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación, por medio de la Organización, ha establecido 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 de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas, ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- 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 de la Agencia Notarial de Certificación.

Estas medidas resultan aplicables a las instalaciones de la Organización donde se realiza la aprobación de las solicitudes de certificados y la gestión de las tarjetas criptográficas bajo la plena responsabilidad de la Agencia Notarial de Certificación.

La Agencia Notarial de Certificación, en las instalaciones de la Organización, ha establecido medidas de seguridad y de protección de datos personales suficientes en relación con los servicios de aprobación, de generación técnica y de manipulado de tarjetas.

7.1.1. Localización y construcción de las instalaciones

En todos los dominios

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta.

Dominio de creación de certificados

La Agencia Notarial de Certificación dispone de instalaciones que protegen físicamente la prestación de los servicio de generación de certificados, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

La localización de las instalaciones permite la presencia de fuerzas de seguridad en un plazo de tiempo razonablemente inmediato desde que una incidencia fuera notificada a los mismos.

La Agencia Notarial de Certificación mantiene instalaciones de recuperación ante desastre para sus operaciones de generación de certificados, con perímetros de seguridad comparables a los de las instalaciones principales.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación, en las instalaciones de la Organización, dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados, de gestión de tarjetas y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

7.1.2. Acceso físico

Dominio de creación de certificados

La Agencia Notarial de Certificación ha establecido 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 donde se llevan a cabo procesos relacionados con el ciclo de vida del certificado, es 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, se realiza mediante técnicas de doble factor de autenticación, incluyendo una tarjeta de proximidad de empleado y códigos PIN, excepto en caso de visitas escoltadas.

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

Los accesos a materiales de claves se encuentran sujetos a una estricta política de segregación de funciones, y la apertura y cierre de dichas cabinas y cajas fuertes se registra para su auditoría posterior.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación, en las instalaciones de las Organizaciones, dispone de la adecuada y suficiente seguridad física para la protección del servicio de aprobación de las solicitudes de certificados y de gestión de las tarjetas criptográficas.

7.1.3. Electricidad y aire acondicionado

En todos los dominios

Los equipos informáticos de la Agencia Notarial de Certificación están convenientemente protegidos ante fluctuaciones o cortes del suministro eléctrico, que pudieran dañarlos o interrumpir el servicio.

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

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

7.1.4. Exposición al agua

En todos los dominios

La Agencia Notarial de Certificación dispone de sistemas de detección de inundaciones adecuados para proteger los equipos y activos ante tal eventualidad.

7.1.5. Prevención y protección de incendios

Dominio de creación de certificados

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

En concreto, los dispositivos criptográficos, y soportes que almacenan claves de las Entidades de Certificación, cuentan con un sistema específico y adicional al resto de la instalación, para la protección frente al fuego.

Dominio de registro de usuario y gestión de tarjetas en la Organización

Todas las instalaciones y activos de la Agencia Notarial de Certificación, en las instalaciones de las Organizaciones, cuentan con sistemas de extinción de incendios, de acuerdo con las normativas locales de prevención de incendios.

7.1.6. Almacenamiento de soportes

En todos los dominios

El almacenamiento de soportes de información garantiza tanto su integridad como su confidencialidad, de acuerdo con la clasificación de la información que se ha establecido.

Se cuenta para ellos con dependencias o armarios ignífugos.

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

7.1.7. Tratamiento de residuos

En todos los dominios

La eliminación de soportes, tanto papel como magnéticos, se realiza mediante mecanismos que garantizan la imposibilidad de recuperación de la información.

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

En el caso de documentación en papel, éste se somete a un tratamiento físico de destrucción.

7.1.8. Copia de respaldo fuera de las instalaciones

En todos los dominios

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

7.2. Controles de procedimientos

En todos los dominios

La Agencia Notarial de Certificación garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

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

7.2.1. Funciones fiables

Dominio de creación de certificados

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

Las personas que deban ocupar tales puestos son formalmente nombradas por la alta dirección de la Agencia Notarial de Certificación.

Las funciones fiables incluyen:

- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.
- Auditores del sistema.
- Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de control específicos.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación, para las instalaciones de las Organizaciones, ha identificado, en su política de seguridad, funciones o roles con la condición de fiables.

Las personas que deban ocupar tales puestos son formalmente nombradas por un representante legal de la Organización.

Las funciones fiables incluyen:

- Personal responsable de la seguridad.
- Personal de atención al cliente.
- Personal de operación criptográfica

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de control específicos.

7.2.2. Número de personas por tarea

Dominio de creación de certificados

Las funciones fiables identificadas en la sección anterior y en la política de seguridad, y sus responsabilidades asociadas, han sido documentadas en descripciones de puestos de trabajo.

Dichas descripciones se han realizado teniendo en cuenta que existe una separación de funciones sensibles, así como una concesión de mínimo privilegio, cuando sea posible.

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

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

- Habilidades requeridas.

Las tareas más sensibles, como el acceso y la gestión del hardware criptográfico de la Entidad de Certificación y las claves asociadas, requiere múltiples personas fiables. En concreto, los procedimientos de control interno han sido diseñados para garantizar que, como mínimo, se requieren dos personas fiables para acceder física o lógicamente al dispositivo.

El acceso al hardware criptográfico de la Entidad de Certificación por parte de múltiples personas fiables se controla de forma estricta a lo largo de todo el ciclo de vida, desde su recepción e inspección hasta su destrucción final, sea ésta física o lógica.

Dominio de registro de usuario y gestión de tarjetas en la Organización

Las funciones fiables identificadas en la política de seguridad del prestador de servicios de certificación, y sus responsabilidades asociadas, se encuentran documentadas en descripciones de puestos de trabajo.

La Agencia Notarial de Certificación, por medio de la Organización, establece, mantiene y ejecuta procedimientos de control rigurosos que garantizan la segregación de funciones basada en las funciones anteriormente indicadas y que se requieren personas fiables para la realización de tareas sensibles.

7.2.3. Identificación y autenticación para cada función

En todos los dominios

La Agencia Notarial de Certificación identifica y autentica al personal antes de acceder a la correspondiente función fiable.

7.2.4. Roles que requieren separación de tareas

Dominio de creación de certificados

Las siguientes tareas son 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, emisión y destrucción de certificados de autoridad de certificación.
- Emisión y revocación de certificados, y el acceso al depósito

Dominio de registro de usuario y gestión de tarjetas en la Organización

- La solicitud de certificados es realizada por el cliente y la aprobación de dicha solicitud va a cargo del Responsable del Servicio de Certificación en la Organización.
- El Responsable del Servicio de Certificación en la Organización realiza la impresión segura y el manipulado de la tarjeta.

7.3. Controles de personal

7.3.1. Requisitos de historial, calificaciones, experiencia y autorización

En todos los dominios

La Agencia Notarial de Certificación emplea 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 aplica al personal de gestión, especialmente en relación con procedimientos de personal de seguridad.

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

El personal en puestos fiables se encuentra libre de intereses personales que entre en conflicto con el desarrollo de la función que tiene encomendada.

No se asigna a un puesto fiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte a su idoneidad para el puesto. Por este motivo, se realiza 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.

7.3.2. Procedimientos de investigación de historial

Dominio de creación de certificados

La Agencia Notarial de Certificación realiza 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 informa acerca de la necesidad de someterse a una investigación previa.

Se advierte de que la negativa a someterse a la investigación implica el rechazo de la solicitud.

Se obtiene consentimiento inequívoco del afectado para la investigación previa y se procesan y protegen todos sus datos personales de acuerdo con la LOPD y el Reglamento que la desarrolla (RD 1720/2007, de 21 de diciembre).

Se realizan las siguientes comprobaciones:

- Referencias a los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada

La investigación se repite cada tres años.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación comprobará la existencia de la Organización y del representante legal autorizado.

7.3.3. Requisitos de formación

En todos los dominios

La Agencia Notarial de Certificación formar al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, de acuerdo con lo establecido en la sección 7.3.1 de esta Declaración de Prácticas de Certificación.

La formación incluye 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.

7.3.4. Requisitos y frecuencia de actualización formativa

En todos los dominios

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

7.3.5. Secuencia y frecuencia de rotación laboral

Dominio de creación de certificados

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

Dominio de registro de usuario y gestión de tarjetas en la Organización

No aplicable

7.3.6. Sanciones para acciones no autorizadas

Dominio de creación de certificados

La Agencia Notarial de Certificación dispone de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, que se encuentra 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 incluyen la suspensión y el despido de la persona responsable de la acción dañina.

Dominio de registro de usuario y gestión de tarjetas en la Organización

No aplicable

7.3.6.1. Procedimiento disciplinario

El personal de Agencia Notarial de Certificación está obligado a cumplir lo siguiente:

- Utilizar los medios materiales de la Agencia Notarial de Certificación sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de la entidad o de terceros, o que puedan atentar contra la moral o las normas deontológicas y de etiqueta de las redes telemáticas.
- No enviar información confidencial al exterior, mediante soportes físicos, o mediante cualquier medio de comunicación, incluyendo la simple visualización o acceso, excepto autorización de Agencia Notarial de Certificación.
- Guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directa o indirectamente ni mediante terceras personas o empresas, los datos, documentos, metodologías, claves, análisis, programas y otra información a la que tengan acceso durante su relación laboral con la Agencia Notarial de Certificación o con instituciones relacionadas o de las que sea miembro la misma, tanto en soporte físico como informático. Esta obligación restará vigente aunque se hubiera extinguido la relación laboral.
- No poseer, para usos no propios de su responsabilidad, ningún material o información propiedad de la Agencia Notarial de Certificación, tanto ahora como en el futuro.
- En el caso que, por motivos directamente relacionados con el puesto de trabajo, entre en posesión de información confidencial bajo cualquier tipo de soporte, dicha posesión deberá entenderse como estrictamente temporal, con la obligación de secreto y sin que tal hecho le otorgue ningún derecho de posesión, o titularidad o copia sobre la referida información. Asimismo, deberá devolver los materiales antes comentados a la Agencia Notarial de Certificación inmediatamente después de la finalización de las tareas que han originado el uso temporal de los mismos, y en cualquier caso, a la finalización de la relación laboral.

- Ceder exclusivamente a la Agencia Notarial de Certificación los derechos de patentes, reproducción e inventos u otra propiedad intelectual que ellos originen y/o desarrollen. Todos los programas y documentación generada por los empleados en su tiempo de trabajo y/o con los medios y/o materiales de la Agencia Notarial de Certificación se consideran propiedad de ésta, la cual asume todos los derechos legales de propiedad de los contenidos de todos los sistemas informáticos bajo su control.

Con el fin de asegurar el cumplimiento de la normativa interna de la Agencia Notarial de Certificación, ésta se reserva el derecho a revisar, sin previo aviso, los sistemas informáticos (archivos de correo electrónico, archivos del disco duro de ordenadores personales, archivos de buzón de voz, colas de impresión, etc..). Las inspecciones se efectúan previa aprobación por el Departamento de Seguridad, de acuerdo con el procedimiento establecido en la normativa aplicable.

La Agencia Notarial de Certificación puede eliminar de su sistema informático cualquier material que considere ofensivo o potencialmente ilegal.

7.3.6.2. Actividades no autorizadas

En materia de seguridad, son actividades no autorizadas para los empleados de la Agencia Notarial de Certificación:

- Compartir o facilitar los identificadores de usuario y/o la clave de acceso facilitados por la Agencia Notarial de Certificación con otra tercera persona, incluido el personal de la misma. En caso de incumplimiento de esta prohibición, el empleado será el único responsable de los actos realizados por la tercera persona que utilice de forma no autorizada el identificador del usuario.
- Intentar distorsionar o falsear los registros LOG del sistema.
- Intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos de la Agencia Notarial de Certificación.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de la Agencia Notarial de Certificación o de terceros.
- Obstaculizar voluntariamente el acceso de otros empleados a la red mediante el consumo masivo de los recursos informáticos y telemáticos de la Agencia Notarial de Certificación, así como realizar acciones que dañen, interrumpan o generen fallos en el sistema.
- Enviar mensajes de correo electrónico de forma masiva o con finalidades comerciales o publicitarias sin el consentimiento del destinatario (Spam).
- Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros empleados.
- Utilizar el sistema para intentar acceder a áreas restringidas de los sistemas informáticos de la Agencia Notarial de Certificación o de terceros.
- Intentar aumentar el nivel de privilegios de un empleado en el sistema.

- Introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que provoquen o sean susceptibles de causar cualquier tipo de alteración en el sistema informático de la Agencia Notarial de Certificación o de terceros. El empleado tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.
- Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos no autorizados expresamente por la Agencia Notarial de Certificación.
- Instalar copias ilegales de cualquier programa, incluidas las estandarizadas.
- Borrar cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de la Agencia Notarial de Certificación incluida la red Internet, para actividades que no estén relacionadas con el lugar de trabajo del empleado.
- Introducir en la red corporativa de la Agencia Notarial de Certificación contenidos obscenos, inmorales u ofensivos y, en general, carentes de utilidad para los objetivos de la misma.
- Acceder y/o utilizar la información sobre personas físicas o jurídicas identificadas o identificables en la red sin la necesaria legitimación para su uso.
- Crear archivos de datos personales sin la autorización de la Agencia Notarial de Certificación.
- Cruzar información relativa a datos personales de diferentes archivos o servicios con la finalidad de establecer perfiles de personalidad, hábitos de consumo o cualquier tipo de preferencias, sin la autorización expresa de la Agencia Notarial de Certificación.
- Cualquier otra actividad expresamente prohibida en la política de Seguridad de la Agencia Notarial de Certificación y en la legislación vigente en materia de protección de datos de carácter personal.
- Tratar datos de carácter personal dentro y fuera del ámbito de tratamiento de la Agencia Notarial de Certificación, en forma escrita o en forma oral, sin contar con la debida legitimación.
- El uso de sistemas de bypass, cuyo objetivo es evitar las medidas de protección, y otros archivos que puedan comprometer los sistemas de protección o los recursos.

7.3.7. Requisitos de contratación de profesionales

Dominio de creación de certificados

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

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

Dominio de registro de usuario y gestión de tarjetas en Organización

No aplicable

7.3.8. Suministro de documentación al personal

Dominio de creación de certificados

La Agencia Notarial de Certificación suministra la documentación que estrictamente precisa su personal en cada momento, al objeto de que sea suficientemente competente a tenor de lo establecido en la sección 7.3.1 de esta Declaración de Prácticas de Certificación.

Dominio de registro de usuario y gestión de tarjetas en la Organización

No aplicable

7.4. Procedimientos de auditoría de seguridad

7.4.1. Tipos de eventos registrados

Dominio de creación de certificados

La Agencia Notarial de Certificación guarda 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 también guarda, 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.

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación por medio de la Organización guarda la siguiente información:

- Encendido y apagado del sistema donde se aloja la entidad de registro.
- Inicio y terminación de la aplicación de entidad de registro.
- Procesamiento correcto e incorrecto de solicitudes.
- Solicitudes de emisión, renovación y revocación de certificados.

7.4.2. Frecuencia de tratamiento de registros de auditoría

En todos los dominios

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

El procesamiento de los registros de auditoría consiste 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.

7.4.3. Periodo de conservación de registros de auditoría

En todos los dominios

Los registros de auditoría se retienen en el recinto durante por lo menos dos meses después de procesarlos y a partir de ese momento se archivan de acuerdo con la sección 7.5.2 de esta Declaración de Prácticas de Certificación.

7.4.4. Protección de los registros de auditoría

En todos los dominios

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

7.4.5. Procedimientos de copia de respaldo

En todos los dominios

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

7.4.6. Localización del sistema de acumulación de registros de auditoría

En todos los dominios

El sistema de acumulación de registros de auditoría es 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 son almacenados por el personal debidamente autorizado.

7.4.7. Notificación del evento de auditoría al causante del evento

En todos los dominios

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

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

7.4.8. Análisis de vulnerabilidades

En todos los dominios

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

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

Estos análisis son 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.

7.5. Archivo de informaciones

En todos los dominios

La Agencia Notarial de Certificación garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 7.5.2 de esta Declaración de Prácticas de Certificación.

7.5.1. Tipos de eventos registrados

Dominio de creación de certificados

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

Se guarda un registro de lo siguiente:

- Identidad de la entidad que procesa la solicitud de certificado.
- Información del ciclo de vida del certificado
- Los datos de auditoría identificados en la sección **¡Error! No se encuentra el origen de la referencia.**

Dominio de registro de usuario y gestión de tarjetas en la Organización

La Agencia Notarial de Certificación, por medio de la Organización, guarda la siguiente información:

- Tipo de documento presentado en la solicitud del certificado.
- Número de identificación único proporcionado por el documento anterior.
- La ubicación de las solicitudes de certificados y del documento firmado por el suscriptor o por el poseedor de las claves, según proceda, documentos que son guardados por el Responsable del Servicio de Certificación de la Organización.

7.5.2. Periodo de conservación de registros

En todos los dominios

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

7.5.3. Protección del archivo

En todos los dominios

La Agencia Notarial de Certificación:

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

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

7.5.4. Procedimientos de copia de respaldo

En todos los dominios

La Agencia Notarial de Certificación realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, según la sección 7.5.1 de esta Declaración de Prácticas de Certificación. Además, realiza copias de respaldo completas semanalmente para casos de recuperación de datos, de acuerdo con la sección 7.7 de esta Declaración de Prácticas de Certificación.

Dominio de creación de certificados

Además, guarda los documentos en papel, según la sección 7.5.1, 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 7.7 de esta Declaración de Prácticas de Certificación.

Dominio de registro de usuario y gestión de tarjetas en la Organización

En este dominio se utilizarán las mismas medidas que las usadas en los procedimientos de la Organización

7.5.5. Requisitos de sellado de fecha y hora

Dominio de creación de certificados

La Agencia Notarial de Certificación emite los certificados y las CRLs con información fiable de fecha y hora, sin que esta información se encuentre firmada digitalmente.

Dominio de registro de usuario y gestión de tarjetas en la Organización

Las bases de datos de la Entidad de Registro emplean registros fiables de fecha y hora.

No es necesario que esta información se encuentre firmada digitalmente.

7.5.6. Localización del sistema de archivo

En todos los dominios

La Agencia Notarial de Certificación dispone de un sistema de mantenimiento de datos de archivo fuera de sus propias instalaciones, tal y como se especifica en la sección 7.5.4 de esta Declaración de Prácticas de Certificación.

7.5.7. Procedimientos de obtención y verificación de información de archivo

En todos los dominios

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

7.6. Renovación de claves

Dominio de creación de certificados

La Agencia Notarial de Certificación ha establecido un plan de renovación programada de las claves de los certificados de infraestructura, que garantiza la continuidad de los servicios.

Dominio de registro de usuario y gestión de tarjetas en la Organización

No aplica

7.7. Compromiso de claves y recuperación de desastre

7.7.1. Procedimientos de gestión de incidencias y compromisos

Dominio de creación de certificados

Se guardan copias de seguridad de la siguiente información de la Agencia Notarial de Certificación, en instalaciones de almacenamiento externo a dicha Agencia Notarial de Certificación, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de base de datos de todos los certificados emitidos.

Las copias de seguridad de las claves privadas de la Agencia Notarial de Certificación son generadas y mantenidas de acuerdo con lo establecido en la sección 8.2.4.

Dominio de registro de usuarios y gestión de tarjetas por la Organización.

Se utilizan las mismas medidas que para la gestión de incidencias en la Organización.

7.7.2. Corrupción de recursos, aplicaciones o datos

Dominio de creación de certificados

Cuando tenga lugar un evento de corrupción de recursos, aplicaciones o datos, la Agencia Notarial de Certificación iniciará 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.

Dominio de registro de usuarios y gestión de tarjetas por la Organización.

Se comunica la incidencia al Responsable de Seguridad de la Organización y se inician los procedimientos de gestión oportunos, que contemplan escalado, investigación y respuesta al incidente.

7.7.3. Revocación de la clave pública de la entidad

Dominio de creación de certificados

En el caso de que la Agencia Notarial de Certificación deba revocar la clave pública de una Entidad de Certificación de su jerarquía, realizará las siguientes acciones:

- Notificar este hecho, cuando se produzca, al Consejo General del Notariado.
- Informar del hecho publicando una CRL, según lo establecido en la sección 6.9.6 de esta Declaración de Prácticas de Certificación.
- 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 7.6 de esta Declaración de Prácticas de Certificación.

Dominio de registro de usuarios y gestión de tarjetas por la Organización.

- No aplicable para este dominio.

7.7.4. Compromiso de la clave privada de la entidad

Dominio de creación de certificados

El plan de continuidad de negocio de la Agencia Notarial de Certificación (o plan de recuperación de desastres) considera 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 realizará 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.

Dominio de registro de usuarios y gestión de tarjetas por la Organización.

- No aplicable para este dominio.

7.7.5. Desastre sobre las instalaciones

Dominio de creación de certificados

La Agencia Notarial de Certificación ha desarrollado, mantiene, prueba y, si es necesario, ejecutará 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 en el menor plazo que resulte posible a tenor de las circunstancias.

La Agencia Notarial de Certificación es capaz de 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 está 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 tienen las medidas de seguridad físicas especificadas en el plan de seguridad, equivalentes a las de las instalaciones principales.

Dominio de registro de usuarios y gestión de tarjetas por la Organización.

- No aplicable para este dominio.

7.8. Terminación del servicio

Dominio de creación de certificados

La Agencia Notarial de Certificación comunicará, en su caso, el cese de su actividad, a los suscriptores que utilicen los certificados electrónicos que haya expedido; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia.

La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.

Asimismo, la Agencia Notarial de Certificación publicará en el web del servicio de certificación y en un periódico de ámbito nacional esta circunstancia con una antelación mínima de dos meses. También comunicará al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior punto, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia.

Comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra la misma.

La Agencia Notarial de Certificación remitirá al Ministerio de Industria, Comercio y Turismo con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a

efectos de lo previsto en el artículo 20.1.f) de la Ley de Firma Electrónica. Este Ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo.

Dominio de registro de usuarios y gestión de tarjetas por la Organización

La Agencia Notarial de Certificación, por medio de la Organización, asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, la Agencia Notarial de Certificación por medio de la Organización, desarrolla un plan de terminación, con las siguientes provisiones:

- Ejecución de 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.

8. Controles de seguridad técnica

La Agencia Notarial de Certificación emplea sistemas y productos fiables, que están protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

8.1. Generación e instalación del par de claves

8.1.1. Generación del par de claves

La Agencia Notarial de Certificación, cuando actúa como Entidad de Certificación raíz, genera y firma su propio par de claves y procede 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 finales con garantía de dispositivo seguro son generadas por la Agencia Notarial de Certificación o por las entidades finales, en dispositivos seguros como tarjetas criptográficas. La creación de las claves pública y privada (2048 bits RSA) la realiza la propia tarjeta internamente, de tal forma que se garantiza tanto la robustez de las claves como la imposibilidad de un compromiso de las mismas en el proceso de generación.

Los pares de claves de las entidades finales sin garantía de dispositivo seguro pueden ser creados por el propio suscriptor / poseedor de las claves en sus sistemas operativos o aplicaciones informáticas o por la Agencia Notarial de Certificación. Cuando las claves sean generadas por Ancert se crearán en formato PKCS#12.

8.1.2. Envío de la clave privada al suscriptor

La clave privada del suscriptor o del poseedor de claves con garantía de dispositivo seguro le es entregada debidamente protegida mediante el dispositivo criptográfico mencionado en la sección anterior.

Cuando las claves sean generadas por la Agencia Notarial de Certificación en formato PKCS#12 se establecerán las medidas de seguridad adecuadas para garantizar su entrega segura al suscriptor / poseedor de las claves.

Cuando la clave es generada por la entidad final esta sección no resulta aplicable.

8.1.3. Envío de la clave pública al emisor del certificado

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

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

Las claves de las Entidades de Certificación son 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 publica 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 establecen medidas adicionales para confiar en los certificados autofirmados, como la comprobación de la huella digital del certificado.

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

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

8.1.5. Tamaños de claves

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

8.1.6. Generación de parámetros de clave pública

Sin estipulación.

8.1.7. Comprobación de calidad de parámetros de clave pública

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

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

Las claves de las Entidades de Certificación se generan en hardware criptográfico que cumple el estándar FIPS 140-2 Nivel 3.

Las claves de firma electrónica reconocida de los usuarios finales se generan en dispositivos criptográficos que cumplen el perfil de protección descrito en la especificación técnica CEN CWA 14169, pudiendo estar certificados de acuerdo con este perfil de protección u otros perfiles de protección equivalentes, tanto de Criterios Comunes como de otros esquemas de certificación internacionalmente reconocidos.

8.1.9. Propósitos de uso de claves

La Agencia Notarial de Certificación incluye la extensión *KeyUsage* en todos los certificados, indicando los usos permitidos de las correspondientes claves privadas, siempre que resulta posible.

8.2. Protección de la clave privada

8.2.1. Estándares de módulos criptográficos

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

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

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

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

Los dispositivos criptográficos quedan almacenados en las dependencias de la Agencia Notarial de Certificación, y para su acceso es necesaria una persona adicional.

8.2.3. Custodia de la clave privada

No se custodian claves privadas del suscriptor.

8.2.4. Copia de respaldo de la clave privada

La clave privada de las Entidades de Certificación cuenta 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 está expresamente autorizado a estos fines, y se limita a aquel que necesite hacerlo.

Los controles de seguridad que se aplican a las copias de respaldo de las Entidades de Certificación son 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.

8.2.5. Archivo de la clave privada

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

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

8.2.6. Introducción de la clave privada en el módulo criptográfico

Las claves privadas se pueden 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 quedan almacenadas en ficheros cifrados con claves fragmentadas y en dispositivos criptográficos (de las que no pueden ser extraídas)

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

8.2.7. Método de activación de la clave privada

La clave privada de cada Entidad de certificación se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 8.2.2.

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

8.2.8. Método de desactivación de la clave privada

Las claves privadas de la Entidad de certificación raíz se desactivan automáticamente cuando se retira el último de los dispositivos utilizados para su activación descrita en la sección 8.2.2.

Las claves privadas de las Entidades de certificación subordinadas se desactivan automáticamente cada vez que se reinicia la aplicación.

Para certificados de firma electrónica reconocida, cuando se retira el dispositivo criptográfico del lector o se desconecta del ordenador, o la aplicación que lo utilice finaliza la sesión, es necesaria nuevamente la introducción del PIN.

8.2.9. Método de destrucción de la clave privada

Para la destrucción de las claves privadas de la Entidad de certificación y de sus datos de activación se procederá a la destrucción física o al borrado a bajo nivel de los dispositivos que

las contengan siguiendo los procedimientos especificados por el fabricante de los mismos. Posteriormente se destruirán de forma segura cualquier copia de seguridad existente.

Para la destrucción de las claves privadas de las entidades finales en hardware se pone a disposición de los subscriptores un servicio de recogida de dispositivos para su destrucción física segura y un software para el borrado seguro de los dispositivos a través de las Entidades de registro y en la Entidad de certificación.

8.3. Otros aspectos de gestión del par de claves

8.3.1. Archivo de la clave pública

Las Entidades de Certificación archivan sus claves públicas de forma permanente, de acuerdo con lo establecido en la sección 7.5 de esta Declaración de Prácticas de Certificación.

8.3.2. Periodos de utilización de las claves pública y privada

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

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

8.4. Datos de activación

8.4.1. Generación e instalación de datos de activación

En los casos en que la Agencia Notarial de Certificación facilita al suscriptor un dispositivo seguro de creación de firma, entonces los datos de activación del dispositivo, son generados de forma segura por la Agencia Notarial de Certificación.

Para realizar una firma o activar la tarjeta es necesario introducir el código secreto de activación (PIN) que solamente debe conocer el poseedor de claves de la tarjeta. Tres intentos consecutivos erróneos en la introducción del PIN provocan un bloqueo de la tarjeta. Para desbloquear la tarjeta, el poseedor de la tarjeta deberá introducir el código PUK y del mismo modo tres intentos consecutivos erróneos en la introducción del PUK provocan el bloqueo irreversible de la tarjeta.

8.4.2. Protección de datos de activación

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

8.4.3. Otros aspectos de los datos de activación

Sin estipulación.

8.5. Controles de seguridad informática

8.5.1. Requisitos técnicos específicos de seguridad informática

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

- Se garantiza 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 garantiza 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 está restringido y estrechamente controlado.
- El personal es identificado y reconocido antes de utilizar aplicaciones críticas relacionadas con el ciclo de vida del certificado.
- El personal es responsable y puede justificar sus actividades, por ejemplo mediante un archivo de eventos.
- Se evita 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 permiten 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) cuenta con un control de accesos para modificaciones o borrado de datos.

8.5.2. Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Agencia Notarial de Certificación son fiables, debiendo acreditarse dicha condición, por ejemplo, mediante una certificación de producto contra un perfil de protección adecuado, conforme a la norma ISO 15408, con nivel EAL4+.

8.6. Controles técnicos del ciclo de vida

8.6.1. Controles de desarrollo de sistemas

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

8.6.2. Controles de gestión de seguridad

La Agencia Notarial de Certificación mantiene un inventario de todos los activos informativos, debidamente clasificados, de acuerdo con sus necesidades de protección, coherente con el análisis de riesgos efectuado.

La configuración de los sistemas se audita de forma periódica, de acuerdo con lo establecido en la sección 10.1.1 de esta Declaración de Prácticas de Certificación.

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

8.6.3. Evaluación del nivel de seguridad del ciclo de vida

El Consejo General del Notariado puede 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.

8.7. Controles de seguridad de red

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

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

8.8. Controles de ingeniería de módulos criptográficos

Se garantiza 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 cumplen los estándares criptográficos de seguridad, que se han indicado en las secciones anteriores.

Los algoritmos de generación de claves están aceptados para el uso de la clave a que están destinados.

9. Perfiles de certificados y listas de certificados revocados

9.1. Perfil de certificado

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

- Número de serie, que es 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 son 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: 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:

- ETSI TS 101 862 v1.3.3 (2006-01): Qualified Certificate Profile, 2006.
- 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 publica los perfiles de certificados en el Depósito indicado en la sección 4.

9.2. Perfil de la lista de revocación de certificados

La Agencia Notarial de Certificación publica los perfiles de listas de revocación de certificados en el Depósito indicado en la sección 4.

10. Auditoría de conformidad

La Agencia Notarial de Certificación realiza 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.

10.1.1. Frecuencia de la auditoría de conformidad

Se realiza 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.

10.1.2. 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 acude 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.

10.1.3. Relación del auditor con la entidad auditada

Las auditorías de conformidad ejecutadas por terceros son practicadas 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.

10.1.4. Listado de elementos objeto de auditoría

Los elementos objeto de auditoría son 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 detallan en el plan de auditoría de la Agencia Notarial de Certificación.

10.1.5. 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 discute, con la entidad que ha ejecutado la auditoría y, en su caso, con el Consejo General del Notariado, las deficiencias encontradas y desarrolla y ejecuta 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 7.7.3 de esta Declaración de Prácticas de Certificación.
- Terminar los servicios de certificación, tal y como se describe en la sección 7.8 de esta Declaración de Prácticas de Certificación.

10.1.6. Tratamiento de los informes de auditoría

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

11. Requisitos comerciales y legales

11.1. Tarifas

11.1.1. Tarifa de emisión o renovación de certificados

La Agencia Notarial de Certificación establece una tarifa por la emisión o por la renovación de los certificados, que es previamente aprobada por el Consejo General del Notariado.

11.1.2. Tarifa de acceso a certificados

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

11.1.3. Tarifa de acceso a información de estado de certificado

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

11.1.4. Tarifas de otros servicios

Sin estipulación.

11.1.5. Política de reintegro

La Agencia Notarial de Certificación dispone de la siguiente política de reintegro de la tarifa:

Cuando una rectificación o modificación de la Declaración de Prácticas de Certificación implique una limitación de los derechos de uso o una restricción sobre el ámbito de aplicación de un certificado en vigor, el suscriptor del mismo puede instar la revocación del mismo y reclamar como máximo el reembolso del precio del certificado.

En los demás casos, el suscriptor no tendrá derecho alguno al reintegro del coste del certificado.

11.2. Capacidad financiera

La Agencia Notarial de Certificación dispone 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 actúa como agente fiduciario ni representante en forma alguna de los usuarios ni de los terceros de confianza en los certificados que emite.

11.2.1. Cobertura de seguro

La Agencia Notarial de Certificación dispone 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 es de al menos 3.000.000 euros.

11.2.2. Otros activos

Sin estipulación.

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

Sin estipulación.

11.3. Confidencialidad

11.3.1. Informaciones confidenciales

Las siguientes informaciones, como mínimo, son 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".

11.3.2. Informaciones no confidenciales

La siguiente información se considera 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 Declaración de Prácticas de Certificación.

11.3.3. Divulgación de información de suspensión y revocación

Véase la sección anterior.

11.3.4. Divulgación legal de información

La Agencia Notarial de Certificación divulga 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 son 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 indican estas circunstancias en la política de intimidad prevista en la sección 11.4 de esta Declaración de Prácticas de Certificación.

11.3.5. Divulgación de información por petición de su titular

La Agencia Notarial de Certificación incluye, en la política de intimidad prevista en la sección 11.4 de esta Declaración de Prácticas de Certificación, 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.

11.3.6. Otras circunstancias de divulgación de información

Sin estipulación.

11.4. Protección de datos personales

Para la prestación del servicio, la Agencia Notarial de Certificación precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales

La Agencia Notarial de Certificación ha desarrollado una política de intimidad, de acuerdo con la Ley Orgánica 15/99, de 13 de diciembre, de Protección de Datos de Carácter Personal, y documenta en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes al documento de seguridad previsto en el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD. Esta Declaración de Prácticas de Certificación tiene la consideración de documento de seguridad.

11.4.1. Ámbito de aplicación de la Protección de Datos

La Agencia Notarial de Certificación protege los Ficheros con datos de carácter personal recogidos en el ejercicio de su actividad como Prestador de Servicios de Certificación (en adelante los Ficheros) de acuerdo con lo previsto en la Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD y demás normativa de desarrollo. Dichos Ficheros son de titularidad privada y su creación, modificación o supresión se notifica al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Para realizar su actividad de certificación las Autoridades de Registro acceden a dichos Ficheros. La Agencia Notarial de Certificación tiene la condición de Responsable del Fichero en tanto que decide sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal y las Entidades de Registro se consideran Encargadas del Tratamiento, las cuales deben utilizar los datos contenidos en dichos Ficheros, única y exclusivamente para los fines que figuran en su Declaración de Prácticas de Certificación.

Las Entidades de Registro, en cumplimiento con lo establecido en el artículo 12 de la LOPD se comprometen a:

1. Tratar los datos personales según las instrucciones del Responsable del Fichero, recibidas en virtud de la relación contractual que les vincula.
2. A garantizar y proteger las libertades públicas y los derechos fundamentales de las personas físicas, y, especialmente, su honor e intimidad personal y familiar.
3. A guardar el secreto profesional respecto de los datos de carácter personal, no divulgando a terceros dicha información obtenida como consecuencia de esta relación contractual, obligación que subsistirá aun después de finalizar sus relaciones con el Responsable del Fichero.
4. A cumplir con todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los Ficheros, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal referidos, reflejado todo ello en el documento de seguridad.
5. A implementar las medidas técnicas y organizativas necesarias que garanticen la seguridad e integridad de los datos de carácter personal incluidos en los Ficheros propiedad del Responsable del Fichero y que eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana, del medio físico o natural.
6. A remitir a la Agencia Notarial de Certificación los datos personales de los solicitantes y/o suscriptores de certificados mediante comunicaciones seguras.
7. A tratar los datos conforme a lo estipulado en el contrato con la Agencia Notarial de Certificación, y no los aplicará o utilizará con fin distinto, ni los comunicará, ni siquiera para su conservación, a otras personas.
8. A acceder únicamente a los Ficheros de la Agencia Notarial de Certificación cuando sea necesario para realizar los servicios contratados.
9. A destruir o devolver todos los datos de carácter personal objeto de tratamiento una vez finalice por cualquier causa la relación con la Agencia Notarial de Certificación, salvo aquellos datos que la legislación obliga a conservarlos por un mínimo de 15 años.

Las entidades de registro verifican que el suscriptor y/o solicitante son informados y prestan su consentimiento para el tratamiento de sus datos, con las finalidades previstas en los documentos de consentimiento correspondiente.

La Agencia Notarial de Certificación queda exonerada de cualquier responsabilidad que se pudiera generar por el incumplimiento por parte de las personas Encargadas del Tratamiento de sus obligaciones descritas. En dichos supuestos de incumplimiento, éstas serán consideradas como responsables del tratamiento y responderán de las infracciones en que hubiese incurrido personalmente.

De conformidad con lo establecido en el artículo 5 de la LOPD, se informa al solicitante/suscriptor que los datos de carácter personal que se incluyan en los formularios, contratos o documentos que cumplimente durante el proceso de solicitud de la emisión de un Certificado se registrarán en un fichero creado al efecto. La Agencia Notarial de Certificación únicamente prestará los servicios de certificación si se cumplimentan los formularios íntegramente con información verdadera. En todo caso, el solicitante/suscriptor que por cualquier medio comunique los datos personales a la Agencia Notarial de Certificación consiente el tratamiento de sus datos para los usos y finalidades de prestar los servicios de certificación en los términos establecidos en la Ley y esta Declaración de Prácticas de Certificación.

De conformidad con lo establecido en el artículo 11 de la LOPD el solicitante/suscriptor, o cualquier usuario de certificados consiente la comunicación a los terceros que confían en certificados electrónicos de sus datos de carácter personal que constan en el certificado a través del Depósito de Cerificados que consta en la página Web www.ancert.com exclusivamente para la finalidad de permitir la consulta de los certificados emitidos por la Agencia Notarial de Certificación y la vigencia de los mismos, así en el Depósito de Certificados y las Listas de Certificados Revocados para consultar los certificados revocados por la Agencia Notarial de Certificación.

Los terceros que confían en certificados únicamente podrán utilizar la información de acuerdo con las finalidades descritas. No obstante, y con carácter general, cualquier tratamiento, registro o utilización para otros fines distintos de los anteriores requiere obligatoriamente del consentimiento previo de los titulares de los datos. Se advierte que la LOPD sanciona con multas que pueden alcanzar los SEISCIENTOS MIL EUROS (600.000€) por cada una de las infracciones o incumplimientos de dicha Ley, sin perjuicio de la incoación de acciones penales de acuerdo con el Código Penal, así como de reclamaciones civiles de los perjudicados.

El solicitante/suscriptor podrá ejercitar los derechos de acceso, rectificación, cancelación y oposición previstos en la LOPD mediante envío de la solicitud a la dirección que aparece en la sección 3.5.2 de esta Declaración de Prácticas de Certificación.

11.4.2. Documento de seguridad

11.4.2.1. Objetivo del Documento de Seguridad

Mediante el presente documento la Agencia Notarial de Certificación establece las medidas de seguridad a implantar para la protección de los datos de carácter personal, contenidos en sus

ficheros que contengan de carácter personal, de acuerdo con la legislación vigente en materia de Protección de Datos de carácter personal.

Como se ha dicho, la Agencia Notarial de Certificación, directamente o a través de las Entidades de Registro, recaba datos de carácter personal de los solicitantes/suscriptores, con el fin de identificarlos y prestarles los servicios de certificación interesados. Dada la naturaleza de este tipo de datos, según indica el Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD, la Agencia Notarial de Certificación debe adoptar medidas de seguridad de nivel básico.

La vigencia del Documento de Seguridad se inicia desde su realización y ordenación de las medidas de seguridad hasta su modificación, en su caso.

Este documento asegura la aplicación de las medidas de índole técnica y organizativa necesarias que garanticen la seguridad de los datos de carácter personal objeto de tratamiento en los Ficheros responsabilidad de la Agencia Notarial de Certificación, para evitar su alteración, pérdida, tratamiento o acceso no autorizado y ser utilizados para una finalidad legítima.

Con el Documento de Seguridad, la Agencia Notarial de Certificación implanta la normativa de seguridad a los equipos y máquinas encargados del tratamiento automatizado de los Ficheros, centros o locales de tratamiento, red, personal, usuarios, puestos de trabajo, programas o aplicaciones y soportes o dispositivos de almacenamiento.

Todo el personal de la Agencia Notarial de Certificación que intervenga directa o indirectamente en el tratamiento automatizado de los datos de carácter personal está obligado a cumplir y a respetar las disposiciones establecidas en el RD 1720/2007, por el que se aprueba el Reglamento de desarrollo de la LOPD y, en especial, lo establecido en el presente documento.

Todo el personal autorizado para acceder a los datos es informado de sus obligaciones y responsabilidades así como del contenido de su contenido.

11.4.2.2. Funciones y obligaciones del personal

El personal de la Agencia Notarial de Certificación como usuarios que tratan los Ficheros conoce y cumple sus funciones y obligaciones establecidas en el Documento de Seguridad de la Agencia Notarial de Certificación. En el uso y tratamiento de los datos de carácter personal del Fichero determinado personal tiene atribuidas funciones diferenciadas, distinguiéndose:

- el Responsable del Fichero

- el Responsable de Seguridad

- el Administrador de Sistemas

Las funciones de estos responsables se definen a continuación:

Responsable del Fichero

Sus funciones pueden ser delegadas en favor del Responsable de Seguridad, constando tal delegación por escrito y firmado expresamente por ambos.

Son funciones propias del Responsable del Fichero:

1. Administrar el Sistema de Protección de Datos personales.
2. Realizar el control del tratamiento, calidad y seguridad de los datos personales.
3. Controlar la forma y requisitos para proceder a los ingresos y cancelaciones.
4. Controlar los soportes de seguridad.
5. Gestionar y dirigir los procedimientos de acceso, rectificación, cancelación y oposición de los afectados.
6. Implantar, dirigir y mantener la política de seguridad y poner los medios necesarios para garantizar el cumplimiento de la normativa vigente respecto del tratamiento de la información sobre personas.
7. Controlar la notificación e inscripción del Fichero.
8. Control de la organización de todo el personal y del cumplimiento por parte de éste de las normas contempladas en el Documento de Seguridad.

Responsable de Seguridad

Será la persona designada formalmente por el responsable de los ficheros para coordinar y controlar las medidas definidas en el documento de seguridad.

Sus funciones son:

• Dentro del ámbito de legalización del Fichero:

1. Legalizar el sistema de información personal y encargarse de que se realicen las notificaciones necesarias ante la Autoridad de Control competente. Asimismo, realizará o supervisará en su caso, que la inscripción del Fichero así como su modificación o cancelación se realicen de forma pertinente.

• Dentro del ámbito de legitimación:

1. Se encarga de que los datos de carácter personal que se incorporen al sistema de información de la Agencia Notarial de Certificación estén debidamente legitimados.
2. Supervisa que la solicitud de los datos cumple con los siguientes principios:
    a. Principio de consentimiento: El tratamiento de los datos de carácter personal, requiere el consentimiento expreso, preciso e inequívoco del titular.
    b. Principio de información: se debe informar previamente al titular de los datos personales de manera expresa, precisa e inequívoca de:
        i. La existencia de un Fichero o tratamiento de datos de carácter personal.
        ii. La identidad y dirección del Responsable del Fichero.
        iii. La finalidad de la recogida.
        iv. Los destinatarios de la información.

v. Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.

vi. Las consecuencias de la obtención de los datos personales y de las consecuencias de la negativa a suministrarlos.

vii. La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

c. Principio de ejercicio: debe garantizarse que el titular de los datos personales pueda ejercer sus Derechos de: Acceso, Rectificación, Cancelación y Oposición

d. Principio de calidad: Los datos de carácter personal sólo se podrán recoger para su tratamiento cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido. Además, los datos deberán ser exactos y puestos al día de forma que respondan con veracidad a la situación actual del titular.

e. Principio de blindaje: El sistema de información deberá quedar blindado, por medio de contratos perimetrales, contra terceros que, en el marco de una relación jurídica de prestación de servicios, accedan o puedan acceder a los datos de carácter personal de los que la Agencia Notarial de Certificación es responsable.

3. Se encarga de la elaboración y mantenimiento del Documento de Seguridad del sistema de información que debe recoger las Medidas de Seguridad en los distintos ámbitos de la entidad

4. Supervisa la correcta aplicación del Documento de Seguridad y del protocolo de registro de incidencias.

• Dentro del ámbito tecnológico sus funciones son:

1. Planificar, ejecutar y controlar las medidas de seguridad de los dispositivos de hardware, software a los distintos aplicativos y comunicaciones, por ello se encarga de:

a) La identificación y autenticación de los usuarios.

b) Del procedimiento de respaldo y recuperación de la Información personal.

c) La organización de los soportes automatizados.

d) Realizar auditorías o revisiones.

e) Controlar las incidencias.

• Dentro del ámbito físico sus funciones son:

1. Planificar, ejecutar y controlar las medidas de seguridad de los centros, las dependencias, los dispositivos de almacenamiento físico y de los soportes físicos, para llevar a cabo todo esto se encarga de:

f) La identificación y autenticación de los usuarios.

g) Del procedimiento de respaldo y recuperación de la Información personal.

h) La organización de los soportes físicos.

i) Realizar auditorías o revisiones.

j) Controlar las incidencias.

Administrador del Sistema

Es la persona encargada de gestionar y mantener el entorno operativo de los ficheros. Con tal finalidad, podrán contar con la posibilidad de acceder a los datos protegidos, previa autorización del Responsable de los Ficheros.

Son funciones propias del Administrador del Sistema de Información:

1. Planificar, ejecutar y controlar las Medidas de Seguridad de los dispositivos de hardware, software a los distintos aplicativos y comunicaciones, por ello se encarga de:
    a) La identificación y autenticación de los Usuarios.
    b) Del procedimiento de respaldo y recuperación de la Información personal.
    c) La organización de los soportes automatizados.
    d) Realizar auditorías o revisiones.
    e) Controlar las incidencias.

11.4.2.3. Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RD 1720/2007.

Centros y zonas de tratamiento

La Agencia Notarial de Certificación dispone de un inventario de accesos físicos en el que se hace referencia a los accesos existentes para acceder a las dependencias en las que se hallan los soportes que facilitan el acceso a la información personal limitando el acceso exclusivamente al personal autorizado.

Los soportes físicos son reordenados y reubicados racionalmente en orden a su criticidad, procurando en la medida de lo posible alojarlos en armarios dotados de cerradura, siguiendo el reglamento de llaves.

Bajo ningún concepto personas no autorizadas podrán permanecer en dependencias que requieran de autorización o habilitación, sin que estén presentes personas autorizadas.

Red, sistema operativo y comunicaciones

La Agencia Notarial de Certificación regula el uso y acceso de los usuarios del sistema operativo, herramientas o programas, o del entorno de comunicaciones, de forma que se impide el acceso no autorizado a la información personal.

Sólo el personal autorizado puede conceder, alterar o anular el acceso autorizado sobre los datos personales y recursos, de conformidad con los criterios establecidos por el Responsable de Seguridad.

El sistema operativo y de comunicaciones está bajo la supervisión del Administrador del Sistema.

El Responsable de Seguridad debe guardar en lugar protegido las copias de seguridad y respaldo, de forma que ninguna persona no autorizada tenga acceso a las mismas.

Sistema Informático o aplicaciones de acceso a la información personal

Los sistemas informáticos de acceso a la información personal deben tener su acceso restringido mediante un código de usuario y una contraseña.

Todos los usuarios autorizados para acceder a la información personal deben tener un código de usuario que será único, y que estará asociado a la contraseña correspondiente, que sólo será conocida por el propio usuario.

Si la aplicación informática que permite el acceso a la información personal no cuenta con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

Las aplicaciones para el tratamiento de datos de carácter personal necesarios para la creación de un certificado electrónico generan ficheros temporales (ficheros de LOGS) los cuales son debidamente custodiados para asegurarse de que esos datos personales no son accesibles posteriormente por personal no autorizado.

Procedimiento de Identificación y Autenticación.

El acceso al servidor de oficina (servidor de dominio) de la Agencia Notarial de Certificación donde está ubicada información personal, está restringido mediante un código de Usuario y una contraseña.

El *Administrador del Sistema* se encarga de que exista una relación actualizada de usuarios que tengan acceso autorizado al sistema de información y de establecer procedimientos de identificación y autenticación para dicho acceso.

Durante el tiempo que estén vigentes, las contraseñas se almacenarán de forma ininteligible.

Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos personales, y deben por tanto estar especialmente protegidas.

Como llaves de acceso al sistema, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al *Responsable de Seguridad* y subsanada en el menor plazo de tiempo posible.

Procedimiento de asignación, distribución y almacenamiento de contraseñas

Existe un procedimiento predeterminado de asignación, distribución y almacenamiento de contraseñas. Sólo las personas que determine el Responsable de Seguridad podrán tener acceso a la información personal del sistema. Las contraseñas se asignarán y se cambiarán mediante el mecanismo y periodicidad determinado en el referido procedimiento.

Los números de identificación y claves de acceso asignadas a cada usuario serán personales e intransferibles, siendo el usuario el único responsable de las consecuencias que puedan derivarse del mal uso, divulgación o pérdida de los mismos.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia y proceder inmediatamente a su cambio.

El archivo donde se almacenen las contraseñas deberá estar protegido y bajo la responsabilidad del Responsable de Seguridad.

11.4.2.4. Estructura del Fichero con datos de carácter personal

La estructura del Fichero de datos de carácter personal utilizado por la Agencia Notarial de Certificación para la finalidad de prestar su actividad de certificación es la que se recoge en el Fichero notificado a la Agencia Española de Protección de Datos. Dicha estructura es la siguiente:

Datos de carácter personal:

- DNI/NIF/Nº pasaporte
- Nombre y apellidos
- Dirección de correo electrónico
- Teléfono
- Domicilio
- Firma electrónica
- Empresa de trabajo
- Atributos (sin poderes, representación de atributos del poseedor de claves bajo la exclusiva autoridad de la Organización)

11.4.2.5. Procedimiento de notificación, gestión y respuesta ante las incidencias

El personal de la Agencia Notarial de Certificación que tenga conocimiento de una incidencia será responsable de la notificación de forma expresa y por escrito al responsable del ámbito al que afecte esa incidencia, ya sea el ámbito físico, el tecnológico o el de recursos humanos.

Se considera incidencia cualquier evento que pueda producirse esporádicamente y que pueda suponer un peligro para la seguridad de los Ficheros, entendida bajo sus tres vertientes de confidencialidad, integridad y disponibilidad de los datos.

El Responsable de Seguridad habilita un Libro registro de incidencias en el que cada uno de los responsables de los diferentes ámbitos, previa notificación expresa y por escrito que deberá realizar cualquier usuario al detectar una incidencia, registrará la citada incidencia en el mismo. Éste anotará dicha incidencia con todos y cada uno de los datos detallados en el párrafo anterior en el libro registro de incidencias.

El conocimiento y la no notificación de una incidencia por parte de un usuario deberán ser considerados como una falta contra la seguridad de los Ficheros.

La notificación de una incidencia deberá constar al menos de los siguientes datos: tipo de incidencia, fecha y hora en que se produjo, persona que realiza la notificación, persona a quien se comunica, efectos que puede producir, descripción detallada de la misma.

11.4.2.6. Procedimientos de copias de seguridad y recuperación de datos

La seguridad de los datos personales del Fichero no sólo supone la confidencialidad de los mismos sino que también conlleva la integridad y la disponibilidad de esos datos.

Para garantizar estos dos aspectos de la seguridad es necesario que existan unos procesos de respaldo y de recuperación que, en caso de fallo del sistema informático, permitan recuperar y en su caso reconstruir los datos de los Ficheros.

El Responsable de Seguridad será responsable de obtener diariamente una copia de seguridad de los Ficheros a efectos de respaldo y posible recuperación en caso de fallo y custodiarla debidamente fuera de las instalaciones.

En caso de fallo del sistema con pérdida total o parcial de los datos personales existirá un Plan de emergencia que consistirá en establecer un procedimiento que partiendo de la última copia de respaldo y del registro de las operaciones realizadas desde el momento de la copia, reconstruya los datos personales al estado en que se encontraban en el momento del fallo.

Será necesaria la autorización por escrito del Responsable de Seguridad para la ejecución de los procedimientos de recuperación de los datos personales, y deberá dejarse constancia en el libro registro de incidencias de las operaciones que hayan debido realizarse para dichas recuperaciones, incluyendo la persona que realizó el proceso, los datos restaurados y los datos que hayan debido ser grabados manualmente en el proceso de recuperación.

11.4.2.7. Gestión de soportes

Los soportes que contengan los Ficheros, bien como consecuencia de operaciones intermedias propias de la aplicación que los trata, o bien como consecuencia de procesos periódicos de respaldo, deberán estar claramente identificados con una etiqueta externa que indique de qué archivo se trata, que tipo de datos contiene, proceso que los ha originado y fecha de creación.

El Responsable de cada ámbito llevará una relación detallada de los soportes que contengan datos personales, se especificará la situación de cada soporte y se actualizará periódicamente.

Los soportes que contengan los Ficheros deberán ser almacenados en lugares a los que no tengan acceso personas no autorizadas para el uso de los mismos.

La salida de soportes que contengan los Ficheros fuera de las dependencias donde está ubicado el sistema de información deberá ser expresamente autorizada por el Responsable de Seguridad utilizando para ello un documento de autorización.

11.5. Derechos de propiedad intelectual

11.5.1. Propiedad de los certificados e información de revocación

La Agencia Notarial de Certificación es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emite, concediendo 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 Declaración de Prácticas de Certificación, según se define en la sección 3.4, y de acuerdo con las correspondientes condiciones generales de uso.

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

Los OID propiedad de la Agencia Notarial de Certificación han sido registrados en la IANA (Internet Assigned Number Authority) bajo la rama 1.3.6.1.4.1., habiéndose asignado el número 18920 (ANCERT), siendo dicha información pública en:

http://www.iana.org/assignments/enterprise-numbers

Igualmente queda prohibido el uso total o parcial de cualquiera de los OID asignados a la Agencia Notarial de Certificación salvo para los usos previstos en los Certificados o en el Depósito de Certificados.

Queda prohibida cualquier extracción y/o reutilización de la totalidad o de una parte sustancial de los contenidos o de las bases de datos que la Agencia Notarial de Certificación pone a disposición de los suscriptores de certificados.

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

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

La Agencia Notarial de Certificación es propietaria de esta Declaración de Prácticas de Certificación.

11.5.3. Propiedad de la información relativa a nombres

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

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 5.1 de esta Declaración de Prácticas de Certificación.

11.5.4. Propiedad de claves

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

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

11.6. Obligaciones y responsabilidad civil

11.6.1. Modelo de obligaciones del prestador de servicios de certificación

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

Es la única entidad responsable del cumplimiento de los procedimientos descritos en esta Declaración de Prácticas de Certificación, incluso cuando una parte o la totalidad de las operaciones sean subcontratadas externamente.

La Agencia Notarial de Certificación presta sus servicios de certificación conforme con esta Declaración de Prácticas de Certificación vigente, en la que se detallan sus funciones, procedimientos de operación y medidas de seguridad.

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

Este requisito se cumple, entre otros medios, mediante un "Texto divulgativo de la política de certificado" aplicable, publicado y transmisible electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

Se vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante condiciones generales de emisión y uso de certificados, que se encuentran en lenguaje escrito y comprensible, y que tienen los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 6.5.1, 6.5.2, 11.2, 11.6.7, 11.6.8, 11.6.9 y 11.6.10 de la presente Declaración de Prácticas de Certificación.
- Indicación de la política aplicable, con indicación de si los certificados se expiden al público y de la necesidad de empleo de dispositivo seguro.
- 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 seguro 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 3.4.2 de esta Declaración de Prácticas de Certificación.
- 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.

La Agencia Notarial de Certificación debe asumir otras obligaciones incorporadas directamente en el certificado o incorporadas por referencia.

11.6.2. 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, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La Agencia Notarial de Certificación, como mínimo, garantiza 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, garantiza 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 6.4 de la presente Declaración de Prácticas 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, garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado reconocido, de acuerdo con el artículo 11 de la Ley 59/2003, de 19 de diciembre.
- La responsabilidad de la Agencia Notarial de Certificación, con los límites legales que se establezcan.

11.6.3. Rechazo de otras garantías

La Agencia Notarial de Certificación rechaza toda otra garantía que no sea legalmente exigible, excepto las contempladas en la sección 11.6.2.

Específicamente, la Agencia Notarial de Certificación no garantiza los algoritmos criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que haya aplicado la diligencia debida según el estado de la técnica en cada momento, y haya actuado conforme a lo dispuesto en la presente Declaración de Prácticas de Certificación y en la Ley 59/2003 y su normativa de aplicación.

11.6.4. Limitación de responsabilidades

La Agencia Notarial de Certificación limita 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 limita 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, de acuerdo con lo establecido en la sección 3.4.2 de esta Declaración de Prácticas de Certificación.

Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del suscriptor. En ningún caso podrá el suscriptor ni los terceros perjudicados reclamar a la Agencia Notarial de Certificación compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los certificados para fines de cifrado.

11.6.5. Cláusulas de indemnidad

11.6.5.1. Cláusula de indemnidad de suscriptor

La Agencia Notarial de Certificación incluye, 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.

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

La Agencia Notarial de Certificación incluye, 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.

11.6.6. Caso fortuito y fuerza mayor

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

11.6.7. Ley aplicable

La Agencia Notarial de Certificación establece, 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.

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

La Agencia Notarial de Certificación establece, 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 11.6.1 (Obligaciones y responsabilidad), 10 (Auditoría de conformidad) y 11.3 (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.

11.6.9. Cláusula de jurisdicción competente

La Agencia Notarial de Certificación establece, 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 determina en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

11.6.10. Resolución de conflictos

La Agencia Notarial de Certificación establece, 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.