DECLARACION DE PRÁCTICAS DE CERTIFICACION (CPS)

Versión 1.1
Fecha: 25/10/2004

Índice

1 INTRODUCCION

1.1. Presentación

El **CONSEJO GENERAL DEL NOTARIADO,** a través de la sociedad mercantil **Agencia Notarial de Certificación, SL Unipersonal** (en adelante **Agencia Notarial de Certificación**)**,** de la que posee el 100% del capital social, se constituye como *Prestador de Servicios de Certificación o Autoridad de Certificación*, considerándose el presente documento como la preceptiva *Declaración de Prácticas de Certificación,* significando que los actos de la segunda se vinculan al primero, el cual responderá de cuantas responsabilidades pueda derivársele a la **Agencia Notarial de Certificación**, en el ejercicio de su función como *Autoridad de Certificación*.

Según dispone el artículo 336 del Reglamento Notarial, el CONSEJO GENERAL DEL NOTARIADO es una Corporación de Derecho Público, con personalidad jurídica propia y plena capacidad, cuyos fines esenciales son:

- Colaborar con la Administración,
- Mantener la organización colegial,
- Coordinar las funciones de los Colegios Notariales, asumiéndolas en los casos legalmente establecidos y,
- Ostentar la representación unitaria del Notariado español.

A estos efectos, el fin esencial del Notariado es la prestación de la seguridad jurídica a que se refiere, como principio rector básico de nuestro ordenamiento jurídico, el artículo 9.3 de la Constitución, siendo así que dicha finalidad se cumple por el Notario, entre otras actuaciones, mediante la dación de fe de la identidad de los otorgantes, de que éstos tienen a juicio del Notario capacidad y legitimación suficiente para la realización del acto o negocio de que se trate, de que el consentimiento ha sido libremente prestado y de que el otorgamiento se adecua a la legalidad y voluntad debidamente informada de los otorgantes o intervinientes.

La presente *Declaración de Prácticas de Certificación* se articula en torno a la Disposición Adicional Primera de la Ley 59/2003 de 19 de diciembre, de *Firma electrónica* (en adelante la *Ley de Firma Electrónica*) que faculta al **CONSEJO GENERAL DEL NOTARIADO** para la emisión de *Certificados* que incorporen *Firma electrónica reconocida* en los términos establecidos en el artículo 3 de la *Ley*.

A efectos organizativos la **Agencia Notarial de Certificación** actuará bajo la responsabilidad de un Director.

La presente *Declaración de Prácticas de Certificación* establece las normas y condiciones generales de los servicios de certificación que presta la **Agencia Notarial de Certificación**, en relación con la gestión de los *Datos de creación y verificación de Firma* y de los *Certificados electrónicos*, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los *Certificados*, las medidas

de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los *Certificados* y los medios que permiten el intercambio de información de forma inmediata sobre la vigencia de los poderes indicados en los *Certificados*, su revocación, sistemas de alertas y comunicaciones notariales en los momentos siguientes a su revocación, y la calificación y suficiencia de las facultades con las que actúen los representantes de las personas jurídicas.

Por tanto, la presente *Declaración de Prácticas de Certificación* se dirige no sólo a los Notarios, sino a todas aquellas personas físicas o jurídicas, *Solicitantes, Suscriptores, Representados*, en general *Usuarios* de los *Certificados* y terceros que confíen en ellos dentro del ámbito que se determina en el presente documento, y en las distintas *Políticas de Certificación* referidas en el presente punto de la *Declaración de Prácticas de Certificación*.

Así, la presente *Declaración de Prácticas de Certificación* constituye, en cumplimiento de lo dispuesto en el artículo 19 de la vigente *Ley de Firma Electrónica*, el compendio general de normas aplicables a toda actividad certificante de la **Agencia Notarial de Certificación** como *Prestador de Servicios de Certificación*. Sin embargo, las distintas especialidades aplicables según los tipos de *Certificados* que se emitan vendrán regidas por las distintas *Políticas de Certificación* que, como normas complementarias y específicas, prevalecerán sobre la presente *Declaración de Prácticas de Certificación* en lo que se refiera a cada *Certificado.* En todo lo no expresamente contemplado en la presente *Declaración de Prácticas de Certificación* o en las *Políticas de Certificación* que la desarrollan se estará a lo dispuesto en la *Ley de Firma Electrónica*.

Los requisitos de la buena fe de los terceros se determinan en el punto 1.3.4 de la presente *Declaración de Prácticas de Certificación*. La **Agencia Notarial de Certificación** solo asumirá las obligaciones y responsabilidades previstas en el presente documento frente a los terceros que reúnan tales requisitos. Los terceros que no reúnan los requisitos indicados no podrán ser considerados de buena fe y en tal caso, la **Agencia Notarial de Certificación** no asumirá ningún compromiso, obligación o responsabilidad frente a ellos.

1.2. Nombre del documento e Identificación

El presente documento se denomina *Declaración de Prácticas de certificación* de la **Agencia Notarial de Certificación, SL Unipersonal**.

OID: 1.3.6.1.4.1.18920.0.1.0.1

1.3. Participantes con la infraestructura de clave pública (PKI)

1.3.1 Prestador de Servicios de Certificación

En la presente *Declaración de Prácticas de Certificación*, se utilizará el acrónimo "ANCERT" para designar en su conjunto, a todas y cada una de las *Autoridades de Certificación raíz* creadas por la **Agencia Notarial de Certificación**, así como a las *Autoridades de Certificación subordinadas* de aquéllas, correspondiendo a todas ellas la calificación, de forma indistinta, de *Prestador de Servicios de Certificación o Autoridad de Certificación.*

1.3.1.1 *Autoridades de Certificación raíz*

Son las *Autoridades de Certificación* que expiden *Certificados raíz* para las *Autoridades de Certificación subordinadas*. La **Agencia Notarial de Certificación** dispone de las siguientes *Autoridades de Certificación raíz*:

- **ANCERT Certificados Notariales**

La *Autoridad de Certificación* **ANCERT Certificados Notariales** se basa en un *Certificado raíz* auto firmado, cuya *huella digital* basada en el algoritmo *SHA-1* es:

C09A B0C8 AD71 1471 4ED5 E21A 5A27 6ADC D5E7 EFCB

- **ANCERT Certificados Redes Privadas**

La *Autoridad de Certificación* **ANCERT Certificados Redes Privadas** se basa en un *Certificado raíz* auto firmado, cuya *huella digital* basada en el algoritmo *SHA-1* es:

04AC 6FE6 22CF F6B1 70EB 7F2D F6A1 3A3B 383E 3D40

- **ANCERT Corporaciones de Derecho Público**

La *Autoridad de Certificación* **ANCERT Corporaciones de Derecho Público** se basa en un *Certificado raíz* auto firmado, cuya *huella digital* basada en el algoritmo *SHA-1* es:

0CFD 83DB AE44 B9A0 C8F6 76F3 B570 650B 94B6 9DBF

- **ANCERT Certificados CGN**

La *Autoridad de Certificación* **ANCERT Certificados CGN** se basa en un *Certificado raíz* auto firmado, cuya *huella digital* basada en el algoritmo *SHA-1* es:

11C5 B5F7 5552 B011 669C 2E97 17DE 6D9B FF5F A810

1.3.1.2 *Autoridades de Certificación subordinadas.*

Son *Autoridades de Certificación* que expiden *Certificados electrónicos* a *Entidades finales* (como se definen en el punto 1.3.3 de esta *Declaración de Prácticas de Certificación*). Cada *Autoridad de Certificación raíz* expide *Certificados raíz* para sus *Autoridades de Certificación subordinadas*. Así:

1. La *Autoridad de Certificación raíz* **ANCERT Certificados Notariales** expide *Certificados raíz* para las siguientes *Autoridades de Certificación subordinadas*:

a) ANCERT Certificados Notariales Personales

Esta *Autoridad de Certificación subordinada* emite los *Certificados electrónicos* denominados *Certificados Notariales Personales*, previa identificación notarial, a personas físicas y a representantes de personas físicas. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificados*.

Existen dos categorías de *Certificados*:

i) Certificados Notariales Personales: Certificados electrónicos emitidos a personas físicas.
ii) *Certificados Notariales Personales de Representación Personal: Certificados electrónicos* emitidos a representantes de personas físicas.

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

9882 F23C 9551 E846 7AE3 3CB2 32DE CE31 41EC 1637

b) ANCERT Certificados Notariales de Sistemas

Esta *Autoridad de Certificación subordinada* emite *Certificados electrónicos* denominados *Certificados Notariales de Sistemas*, previa identificación notarial, a servidores informáticos. Existen cuatro categorías de *Certificados*:

i) *Certificados Notariales de Servidor Seguro*: *Certificados electrónicos* emitidos a servidores *SSL*.
ii) *Certificados Notariales de Sellado de Tiempo*: *Certificados electrónicos* emitidos a servidores de *Sellado de Tiempo*.
iii) *Certificados Notariales de OCSP Responder*: *Certificados electrónicos* emitidos a servidores *OCSP Responder*.
iv) *Certificados Notariales de Servidor Persona Jurídica*: *Certificados electrónicos* emitidos a servidores de aplicaciones para la realización de respuestas automáticas firmadas digitalmente.

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

AA43 237C 5A92 CC2D 32F9 2D5A 2222 4673 755E FDA3

c) ANCERT Certificados Notariales Corporativos

Esta *Autoridad de Certificación subordinada* emite *Certificados electrónicos* denominados *Certificados Notariales Corporativos*, previa identificación notarial, a personas jurídicas y a representantes de personas jurídicas. Se

utilizan *Tarjetas Criptográficas* o *Módulos Criptográficos* como únicos soportes de los *Certificado*s.

Existen dos tipos de *Certificado*s:

i) *Certificados Notariales Corporativos: Certificados electrónicos* emitidos a personas jurídicas.
ii) *Certificados Notariales Corporativos de Representación: Certificados electrónicos* emitidos a representantes de personas jurídicas.

La *huella digital* de esta *Autoridad de Certificación* s*ubordinada* basada en el algoritmo *SHA-1* es:

ADA2 8F80 0D0D 32EA B81E A81C ACAB FE3C 5D09 E45F

2. La *Autoridad de Certificación raíz* **ANCERT Certificados Redes Privadas** emite *Certificado*s *raíz* para la siguiente *Autoridad de Certificación* s*ubordinada*:

a) ANCERT Certificados Corporativos Personales

Esta *Autoridad de Certificación* s*ubordinada* emite *Certificado*s *electrónicos* a personal de una corporación privada. Se denominan *Certificados Corporativos Personales*. La propia empresa es la responsable del registro de sus usuarios, actuando como *Autoridad de Registro*. Este tipo de *Certificado*s son válidos únicamente para su uso en el ámbito interno de la corporación. Se utilizarán *Tarjetas Criptográficas* como único soporte de los *Certificado*s.

La *huella digital* de esta *Autoridad de Certificación* s*ubordinada* basada en el algoritmo *SHA-1* es:

0CA8 54B2 F455 E5F5 34D7 0179 160F 6A2F A66A 9AA2

3. La *Autoridad de Certificación raíz* **ANCERT Corporaciones de Derecho Público** emite *Certificado*s *raíz* para la siguiente *Autoridad de Certificación* s*ubordinada*:

a) ANCERT Certificados para Corporaciones de Derecho Público

Esta *Autoridad de Certificación subordinada* emite *Certificado*s *electrónicos* al personal y a los colegiados de una Corporación de Derecho Público. Se denominan *Certificado*s *Corporativos de Corporaciones de Derecho Público*. El propio Colegio será el responsable del registro de sus colegiados y personal, actuando como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificado*s.

La *huella digital* de esta *Autoridad de Certificación* s*ubordinada* basada en el algoritmo *SHA-1* es:

F280 DF44 3D7A 1417 DE4B B06D C88A 5199 54ED 7AEF

4. La *Autoridad de Certificación raíz* **ANCERT Certificados CGN** emite *Certificado*s *raíz* para la siguiente *Autoridad de Certificación subordinada*:

a) ANCERT Certificados FERN

Esta *Autoridad de Certificación subordinada* emite *Certificados electrónicos* para todos los Notarios establecidos en territorio español. Se denominan *Certificados FERN*. Cada Colegio Notarial del territorio español es el responsable del registro de sus colegiados, actuando como *Autoridad de Registro*. Por su parte el Presidente de la Junta de Decanos actúa como *Autoridad de Registro* para todos los Decanos del territorio español. Se utilizan Tarjetas *Criptográficas* como único soporte de los *Certificado*s.

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

BB5A 6CDF 6882 BDA1 9DFC 8260 5911 BA96 3BB0 A651

b) ANCERT Certificados para Empleados

Esta *Autoridad de Certificación subordinada* emite *Certificados electrónicos* para los empleados de Notarías y Colegios Notariales. Se denominan *Certificados para empleados*. Cada Colegio Notarial es el responsable del registro de sus empleados, actuando como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificado*s.

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

3EA6 664E FA99 BA8F 706A 6B21 9A7F 4983 AD0E E034

1.3.2 Autoridades *de Registro*

Las *Autoridades de Registro* son personas físicas o jurídicas a las que ANCERT encarga la identificación y comprobación de las circunstancias personales de los solicitantes de los *Certificado*s. A tal efecto, las *Autoridades de Registro* se encargarán de garantizar que la solicitud del *Certificado* contiene información veraz y completa del *Solicitante*.

Una vez realizada la referida identificación y comprobación, las *Autoridades de Registro* entregarán a los *Solicitantes* los *Certificado*s, validando y conservando la documentación acreditativa de la información aportada por el *Solicitante*.

1.3.3 Entidades finales

Las *Entidades finales o Usuarios* son las personas físicas o jurídicas que tienen capacidad para solicitar y obtener un *Certificado* electrónico en las condiciones que se

establecen en la presente *Declaración de Prácticas de Certificación* y en las *Políticas de Certificación* vigentes para cada tipo de *Certificado*.

A los efectos de la presente *Declaración de Prácticas de Certificación*, y de las *Políticas de Certificación* que la desarrollan, son *Entidades finales* del sistema de certificación de ANCERT las siguientes:

- *Solicitante*
- *Suscriptor*
- *Representado*

1.3.3.1 Solicitante

Solicitante es la persona física que, en nombre propio o en representación de tercero, y previa identificación, solicita la emisión de un *Certificado*.

En el caso de tratarse de un *Solicitante* de *Certificado* cuyo *Suscriptor* sea una persona jurídica (denominándose *Solicitante/Custodio*) dicha persona física sólo podrá ser un administrador o un representante, legal o voluntario con poder bastante a estos efectos, de la persona jurídica que vaya a ser el *Suscriptor* del *Certificado.*

En el caso de tratarse de un *Solicitante* de *Certificado* cuyo *Suscriptor* sea el propio *Solicitante* (denominándose *Solicitante/Delegante*), pero que solicite que el *Certificado* recoja el ámbito de representación de otra persona física o jurídica, y que el *Certificado* le permita actuar en el ámbito de la Sociedad de la Información haciendo valer las facultades de representación de que dispone, dicha persona física sólo podrá ser un administrador o un representante, legal o voluntario con poder bastante a estos efectos. En cuanto al ámbito de las facultades que podrán ser ejercitadas mediante el uso del *Certificado* no podrán, en ningún caso, ser superiores a las que se tengan delegadas formalmente en el documento público del que traiga causa la concesión de *Firma electrónica* para el *Suscriptor.* El *Suscriptor* de este tipo de *Certificado*s, y de acuerdo con lo prevenido en la vigente Ley de *Firma electrónica*, recibirá la denominación de *Suscriptor*.

También tendrá la condición de *Solicitante* el representante de una persona jurídica que en el ámbito de su representación solicite *Certificado*s para otras personas físicas a las que previamente se les haya delegado por documento público todas o algunas de las facultades del *Solicitante*. El *Solicitante* comparecerá, en tal caso, ante la *Autoridad de Registro*, identificando a las personas físicas que vayan a resultar titulares de los *Certificado*s y que ostentarán en la terminología de la presente *Declaración de Prácticas de Certificación* la condición de *Suscriptores*. Los *Certificado*s se solicitarán para éstos, en función del ámbito de representación que tengan previamente concedido en los documentos públicos de los que resulte su representación, y dentro de las facultades de delegación de facultades que ostente la persona que actúe como solicitante. Las facultades de representación que recojan directa o indirectamente los *Certificado*s tendrán que corresponderse, como máximo, con las que ostenten los suscriptores en los documentos públicos de los que traigan causa. En la concesión, el Notario comprobará, igualmente, que el *Solicitante* actuó como representante de la persona jurídica poderdante en el momento de otorgarse el apoderamiento en virtud del cual se concede el *Certificado*.

En ningún caso se emitirán *Certificado*s para menores de edad.

1.3.3.2 Suscriptor

A los efectos de la presente *CPS*, el *Suscriptor* de los *Certificados* de ANCERT se corresponde con el término *Firmante* previsto en el artículo 6 de la *Ley 59/2003 de Firma Electrónica*.

Tendrá la consideración de *Suscriptor* el titular del *Certificado*. Es la persona física o jurídica cuya identidad personal queda vinculada a los *Datos de creación y verificación de Firma*, firmados electrónicamente, a través de una C*lave Pública* certificada por el *Prestador de Servicios de Certificación*. El concepto de *Suscriptor*, será referido en los *Certificados* y en las aplicaciones informáticas relacionadas con su emisión como *Subject* por razones de estandarización internacional.

En el caso de que el *Suscriptor* sea una persona jurídica resulta directamente vinculada por su uso cuando es ejercido dentro de los límites señalados en su expedición y en el ámbito que constituye su giro o tráfico ordinario, y en cualquier caso cuando los actos realizados con el *Certificado* se hayan celebrado en interés de la misma.

1.3.3.3 Representado

Tendrá la consideración de *Representado* la persona física o jurídica en cuyo nombre un *Solicitante* solicita un *Certificado*.

1.3.4 Terceros que confían en Certificados

Tendrán la consideración de *Terceros que confían en Certificados* expedidos por ANCERT, los que depositan de buena fe su confianza en un *Certificado* de ANCERT, comprobando la validez y vigencia del *Certificado* según lo descrito en esta *Declaración de Prácticas de Certificación*.

1.4. Tipo de Certificados y límites para su uso

1.4.1 *Certificados raíz*

Las *Autoridades de Certificación raíz* de ANCERT descritas en el punto 1.3.1.1 expiden *Certificados raíz* exclusivamente a las *Autoridades de Certificación subordinadas* de la jerarquía de ANCERT.

Los *Certificados raíz* se expiden con la finalidad de que las *Autoridades de Certificación subordinadas* expidan *Certificados* a *Entidades finales*.

1.4.2 *Certificado*s Notariales Personales

La *Autoridad de Certificación subordinada* **ANCERT Certificados Notariales Personales** expide los *Certificado*s *Notariales Personales* a personas físicas, en su nombre propio, previa identificación ante Notario, el cual actuará como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificado*s. Podrán contener o no atributos cumpliendo los requisitos señalados en esta *Declaración de Prácticas de certificación*.

Los *Certificado*s *Notariales Personales* son *Certificado*s *electrónicos reconocidos* utilizados para generar la *Firma electrónica reconocida*, lo cual garantiza la identidad del *Suscriptor* del *Certificado*. La *Firma electrónica reconocida* es la *Firma electrónica* avanzada basada en un *Certificado* reconocido y que ha sido generada 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. Los *Certificado*s *Notariales Personales* incluyen los datos que exige el artículo 11 de la *Ley de Firma electrónica*.

1.4.3 Certificados Notariales Personales de Representación Personal

La *Autoridad de Certificación subordinada* **ANCERT *Certificado*s Notariales Personales** expide los *Certificado*s *Notariales Personales de Representación Personal* a personas físicas en representación de otra persona física, previa identificación ante Notario, el cual actuará como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificado*s. Podrán contener o no atributos cumpliendo los requisitos señalados en esta *Declaración de Prácticas de certificación*.

Los *Certificado*s *Notariales Personales de Representación Personal* son *Certificado*s *electrónicos reconocidos* utilizados para generar la *Firma electrónica reconocida*, lo cual garantiza la identidad del *Suscriptor* del *Certificado*. La *Firma electrónica reconocida* es la *Firma electrónica avanzada* basada en un *Certificado reconocido* y que ha sido generada 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. Los *Certificado*s *Notariales Personales de Representación Personal* incluyen los datos que exige el artículo 11 de la *Ley de Firma electrónica*.

1.4.4 Certificados Notariales Corporativos

La *Autoridad de Certificación subordinada* **ANCERT *Certificado*s Notariales Corporativos** expide los *Certificado*s *Notariales Corporativos* a personas jurídicas, previa identificación ante Notario, el cual actuará como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* y Módulos Criptográficos como únicos soportes de los *Certificado*s.

Los *Certificados Notariales Corporativos*, que se corresponden con los certificados de persona jurídica regulados en el artículo 7 de la Ley 59/2003, se utilizan para la Firma electrónica en el ámbito de las Administraciones Públicas y en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario, entendiendo por tal, las transacciones efectuadas mediata o inmediatamente para la realización del núcleo de la actividad de la entidad y las actividades de gestión o administrativas necesarias para el desarrollo de la misma, como la contratación de suministros tangibles e intangibles o de servicios auxiliares garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido.

1.4.5 Certificados Notariales Corporativos de Representación

La *Autoridad de Certificación subordinada* **ANCERT Certificados Notariales Corporativos** expide los *Certificados Notariales Corporativos de Representación* a personas físicas que actúan en representación de personas jurídicas, confirma la identidad de su *Suscriptor* y determina su capacidad de representar a la persona jurídica, previa identificación ante Notario, el cual actuará como *Autoridad de Registro* y comprobará los datos relativos a la personalidad jurídica del *Representado* y a la extensión y vigencia de las facultades del representante, de acuerdo con lo previsto en al *Ley de Firma electrónica*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificados*.

En los *Certificados Notariales Corporativos de Representación* la persona física deberá aparecer como *Suscriptor* del *Certificado*, e identificado por su nombre, apellidos, NIF, pasaporte o u otro medio admitido en derecho según lo que se establece en esta *CPS*. En este supuesto la persona jurídica deberá figurar como *Representado*, identificada por medio de su razón social o denominación, NIF o datos de su registro administrativo cuando se trate de personas jurídicas constituidas con arreglo a la legislación extranjera, o no residentes en territorio español.

Los *Certificados Notariales Corporativos de Representación* son *Certificados electrónicos reconocidos* y son utilizados para generar la *Firma electrónica reconocida* que garantiza la identidad del *Suscriptor* del *Certificado*, de acuerdo con lo establecido por los artículos 11 y siguientes de la *Ley de Firma electrónica*. Los *Certificados Notariales Corporativos de Representación* se utilizan con dispositivos seguros de creación de *Firma electrónica*.

1.4.6 Certificados Notariales de Servidor Seguro

La *Autoridad de Certificación subordinada* **ANCERT Certificados Notariales de Sistemas** emite los *Certificados Notariales de Servidor Seguro*, previa identificación ante Notario quien actúa como *Autoridad de Registro*, a personas físicas o jurídicas en calidad de titulares del nombre de dominio de servidores *SSL*. Los *Certificados Notariales de Servidor Seguro* son *Certificados electrónicos reconocidos* y se usan para establecer comunicaciones seguras y autenticadas entre servidor y cliente *SSL*.

1.4.7 Certificados Notariales de Sellado de Tiempo

La *Autoridad de Certificación subordinada* **ANCERT Certificados Notariales de Sistemas** emite los *Certificados Notariales de Sellado de Tiempo*, previa identificación ante Notario quien actúa como *Autoridad de Registro*, a personas jurídicas en calidad de titular del servidor de sellado de tiempo. Los *Certificados Notariales de Sellado de Tiempo* son *Certificados electrónicos* que se usan para generar de sellos de tiempo. Se utilizan *Módulos Criptográficos Hardware de Seguridad* como único soporte de los *Certificados*.

1.4.8 Certificados Notariales de OCSP Responder

La *Autoridad de Certificación Subordinada* **ANCERT Certificados Notariales de Sistemas** emite los *Certificados Notariales de OCSP Responder*, previa identificación ante Notario quien actúa como *Autoridad de Registro*, a personas jurídicas en calidad de titulares del *OCSP Responder*. Los *Certificados Notariales de OCSP Responder* son *Certificados electrónicos reconocidos* y se usan para la *Firma electrónica reconocida* de respuestas OCSP. Se utilizan *Módulos Criptográficos Hardware de Seguridad* como único soporte de los *Certificados*.

1.4.9 Certificados Notariales de Servidor Persona Jurídica

La *Autoridad de Certificación subordinada* **ANCERT Certificados Notariales de Sistemas** expide los *Certificados Notariales de Servidor Persona Jurídica* a personas jurídicas, previa identificación ante Notario, el cual actuará como *Autoridad de Registro*. Se utilizan *Módulos Criptográficos Hardware de Seguridad* como único soporte de los *Certificados*.

Los *Certificados Notariales de Servidor Persona Jurídica* vinculan a su *Suscriptor* unos *Datos de Verificación de Firma* y confirman su identidad. Los *Certificados Notariales de Servidor Persona Jurídica* son *Certificados electrónicos reconocidos* utilizados para generar la *Firma electrónica reconocida* en procesos automáticos, en particular para la emisión de facturas electrónicas, en las relaciones que mantenga la persona jurídica con las Administraciones públicas, o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

1.4.10 Certificados Corporativos Personales

La *Autoridad de Certificación subordinada* **ANCERT Certificados Corporativos Personales** emite los *Certificados Corporativos Personales* al personal empleado de una corporación o persona jurídica privada. La propia entidad es la responsable del registro de sus usuarios, actuando como *Autoridad de Registro*. Este tipo de *Certificados electrónicos* son válidos únicamente para su uso en el ámbito interno de la corporación. Se utilizarán *Tarjetas Criptográficas* como único soporte de los *Certificados*.

Estos *Certificados* se consideran de uso privado de la propia corporación o de ésta con otras con las que firme el correspondiente Convenio. Su concesión, uso y revocación vendrán determinados por el marco contractual que rija las relaciones entre la corporación y los titulares de los *Certificados*.

Los *Certificados Corporativos Personales* son *Certificados electrónicos* para generar la *Firma electrónica avanzada* que garantiza la identidad del *Suscriptor* del *Certificado*, de acuerdo con lo establecido por los artículos 11 y siguientes de la *Ley de Firma electrónica*. Los *Certificados Corporativos Personales* se utilizan con dispositivos seguros de creación de *Firma electrónica*.

1.4.11 Certificados Corporativos de Corporaciones de Derecho Público

La *Autoridad de Certificación subordinada* **ANCERT Corporaciones de Derecho Público** emite los *Certificados Corporativos de Corporaciones de Derecho Público* a personal y colegiados de una corporación de derecho público. El propio colegio o corporación será el responsable del registro de sus colegiados y personal, actuando como *Autoridad de Registro*. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificados*.

Los *Certificados Corporativos de Corporaciones de Derecho Público* son *Certificados electrónicos reconocidos* y son utilizados para generar la *Firma electrónica reconocida* que garantiza la identidad del *Suscriptor* del *Certificado*, de acuerdo con lo establecido por los artículos 11 y siguientes de la *Ley de Firma electrónica*. Los *Certificados Corporativos de Corporaciones de Derecho Público* se utilizan con dispositivos seguros de creación de *Firma electrónica*.

1.4.12 Certificados FEREN

La *Autoridad de Certificación subordinada* **ANCERT Certificados FERN** emite los *Certificados FEREN* para todos los Notarios establecidos en territorio español. Cada Colegio de Notarios es el responsable del registro de sus colegiados, actuando como *Autoridad de Registro*. Por su parte el Presidente de la Junta de Decanos actúa como *Autoridad de Registro* para todos los Decanos del territorio español. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificados*.

Los documentos *electrónicos* firmados con este tipo de *Certificados* son los únicos que servirán para la comunicación de los documentos públicos en los términos prevenidos en el artículo 3, número 6, a) de la *Ley de Firma electrónica*.

Los *Certificados FEREN* son *Certificados electrónicos reconocidos* y son utilizados para generar la *Firma electrónica* que garantiza la identidad del *Suscriptor* del *Certificado*, de acuerdo con lo establecido por los artículos 11 y siguientes de la *Ley de Firma electrónica* y lo dispuesto en los artículos 110 y siguientes de la Ley 24/2001. Los *Certificados FEREN* se utilizan con dispositivos seguros de creación de *Firma electrónica*.

1.4.13 Certificados para empleados

La *Autoridad de Certificación* s*ubordinada* **ANCERT Certificados para Empleados** emite los *Certificados para empleados* para los empleados de Notarías y Colegios de Notarios. Cada Notario es el responsable del registro de sus empleados. Por su parte, las Juntas Directivas de los Colegios Notariales serán los responsables del registro de los empleados de los respectivos Colegios. Se utilizan *Tarjetas Criptográficas* como único soporte de los *Certificado*s.

Los *Certificados para empleados* son *Certificados electrónicos reconocidos* y son utilizados para generar la *Firma Electrónica reconocida* que garantiza la identidad del *Suscriptor* del *Certificado*, de acuerdo con lo establecido por los artículos 11 y siguientes de la *Ley de Firma electrónica*. Los *Certificados para empleados* se utilizan con dispositivos seguros de creación de *Firma electrónica*.

1.5. Usos prohibidos de los Certificados

Los *Certificado*s emitidos por ANCERT se utilizarán únicamente conforme a la función y finalidad que tengan establecida en la presente D*eclaración de Prácticas de Certificación* y en las correspondientes *Políticas de Certificación*, y con arreglo a la normativa vigente.

1.6. Tarifas por la expedición de Certificados

Las tarifas vigentes en cada momento por la expedición de *Certificado*s serán puestas a disposición de los *Solicitantes/Suscriptores* por cada *Autoridad de Certificación* de ANCERT.

1.7. Administración de la política

1.7.1 Persona de contacto

Cualquier contacto con la **Agencia Notarial de Certificación**, referente a esta *Declaración de Prácticas de Certificación* puede realizarse vía e-mail a la dirección de correo electrónico ancert@ancert.com, o por teléfono al número 902 348 347 o directamente en la sede central de la **Agencia Notarial de Certificación**:

Agencia Notarial de Certificación, S.L. Unipersonal
Avenida de Martínez Campos, número 46.- 6º, Edificio Elcano
28010 Madrid (España)

Las alteraciones que se produzcan sobre los anteriores datos como *Web*, correo, dirección o teléfono constarán debidamente reflejadas en la *Web* www.ancert.com que ANCERT mantiene en vigor en Internet.

1.7.2 Persona que determina la idoneidad de la Declaración de Prácticas de Certificación

La persona que determina la idoneidad de la *Declaración de Prácticas de Certificación* es el Consejo de Administración de la **Agencia Notarial de Certificación**.

1.7.3 Procedimientos de aprobación de la Declaración de Prácticas de Certificación

El Consejo de Administración de la Agencia Notarial de Certificación es el encargado de aprobar la presente *Declaración de Prácticas de Certificación*.

1.7.4 Procedimiento de modificación de la Declaración de Prácticas de Certificación

La presente *Declaración de Prácticas de Certificación* podrá 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 podrá instar la revocación de su *Certificado*. La revocación así solicitada no dará derecho a reclamar indemnización alguna, ni aun la devolución parcial del precio del *Certificado*, salvo que la 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 del respectivo *Certificado*.

1.8. Definiciones y acrónimos

1.8.1 Definiciones

A los efectos de determinar el alcance de los conceptos que son utilizados en la presente *Declaración de Prácticas de Certificación*, y en las distintas *Políticas de Certificación*, deberá entenderse:

- *Agencia Española de Protección de Datos*: Ente de Derecho Público, con personalidad jurídica propia y plena capacidad pública y privada cuya finalidad es velar por el cumplimiento de la legislación sobre protección de datos personales.
- *Autoridad de Certificación*: es aquella persona física o jurídica que, de conformidad con la legislación sobre *Firma electrónica* expide *Certificados electrónicos*, pudiendo prestar además otros servicios en relación con la *Firma electrónica*. A efectos de la presente *Declaración de Prácticas de Certificación*, son *Autoridad de Certificación* todas aquellas que en la misma se definan como tales.
- *Autoridad de Registro*: persona física o jurídica que ANCERT designa para realizar la comprobación de la identidad de los *Solicitantes y Suscriptores* de *Certificados,* y en su caso de la vigencia de facultades de representantes y subsistencia de la personalidad jurídica o de la representación voluntaria.

- *Cadena de certificación*: lista de *Certificados* que contiene al menos un *Certificado* y el *Certificado raíz* de ANCERT.
- *Certificado*: documento electrónico *firmado electrónicamente* por un *Prestador de Servicios de Certificación* que vincula al *Suscriptor* unos *Datos de verificación de Firma* y confirma su identidad. En la presente *Declaración de Prácticas de Certificación*, cuando se haga referencia a *Certificado* se entenderá realizada a un *Certificado* emitidos por cualquier *Autoridad de Certificación* de ANCERT.
- *Certificado raíz*: *Certificado* cuyo *Suscriptor* es una *Autoridad de Certificación* perteneciente a la jerarquía de ANCERT como *Prestador de Servicios de Certificación,* y que contiene los *Datos de verificación de Firma* de dicha *Autoridad* firmado con los *Datos de creación de Firma* de la misma como *Prestador de Servicios de Certificación*.
- *Certificado reconocido*: *Certificado* expedido por un *Prestador de Servicios de Certificación* que cumple los requisitos establecidos en la 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 presten.
- *Clave*: secuencia de símbolos.
- *Datos de creación de Firma (Clave Privada)*: son datos únicos, como códigos o claves criptográficas privadas, que el signatario utiliza para crear la *Firma electrónica*.
- *Datos de verificación de Firma (Clave Pública)*: son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la *Firma electrónica*.
- *Declaración de Prácticas de Certificación*: declaración de ANCERT puesta a disposición del público por vía electrónica y de forma gratuita realizada en calidad de *Prestador de Servicios de Certificación* en cumplimiento de lo dispuesto por la Ley.
- *Dispositivo seguro de creación de Firma*: instrumento que sirve para aplicar los *Datos de creación de Firma* cumpliendo con los requisitos establecidos en el Anexo III de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999, y con lo establecido en las normas específicas de aplicación en España.
- *Directorio de Certificados*: repositorio de información que sigue el estándar X.500 del ITU-T.
- *Documento electrónico*: conjunto de registros lógicos almacenado en soporte susceptible de ser leído por equipos *electrónicos* de procesamiento de datos, que contiene información.
- *Documento de seguridad*: documento exigido por la LOPD cuyo objetivo es establecer las medidas de seguridad implantadas, a los efectos de este documento, por ANCERT como *Prestador de Servicios de Certificación*, para la protección de los datos de carácter personal contenidos en los *Ficheros* de la actividad de certificación que contienen datos personales (en adelante los *Ficheros*).
- *Encargado del Tratamiento*: la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que trate datos personales por cuenta del Responsable del tratamiento de los *Ficheros*.
- *Firma electrónica reconocida*: es aquella *Firma electrónica avanzada* basada en un *Certificado reconocido* y generada mediante un *Dispositivo seguro de creación de Firma*.
- *Firma electrónica avanzada*: es aquella *Firma electrónica* que permite establecer la identidad personal del *Suscriptor* respecto de los datos firmados y comprobar la integridad de los mismos, por estar vinculada de manera

exclusiva tanto al *Suscriptor,* como a los datos a que se refiere, y por haber sido creada por medios que éste puede mantener bajo su exclusivo control.

- F*irma electrónica*: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación personal.
- *Función hash*: es una operación que se realiza sobre un conjunto de datos de cualquier tamaño, de forma que el resultado obtenido es otro conjunto de datos de tamaño fijo, independientemente del tamaño original, y que tiene la propiedad de estar asociado unívocamente a los datos iniciales, es decir, es imposible encontrar dos mensajes distintos que generen el mismo resultado al aplicar la *Función hash*.
- *Hash o Huella digital*: resultado de tamaño fijo que se obtiene tras aplicar una *Función hash* a un mensaje y que cumple la propiedad de estar asociado unívocamente a los datos iniciales.
- *Infraestructura de Claves Públicas* (PKI, *public key infrastucture*): infraestructura que soporta la gestión de *Claves Públicas* para los servicios de autenticación, cifrado, integridad, o no repudio.
- *Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal*: ley que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
- *Listas de Revocación de Certificados o Listas de Certificados Revocados*: lista donde figuran exclusivamente las relaciones de *Certificados* revocados o suspendidos (no los caducados).
- *Módulo Criptográfico Hardware de Seguridad:* módulo *hardware* utilizado para realizar funciones criptográficas y almacenar *Claves* en modo seguro.
- *Número de serie de Certificado*: valor entero y único que está asociado inequívocamente con un *Certificado* expedido por ANCERT.
- *OCSP (Online Certificate Status Protocol):* protocolo informático que permite la comprobación del estado de un *Certificado* en el momento en que éste es utilizado.
- *OCSP Responder:* servidor informático que responde, siguiendo el protocolo *OCSP*, a las *Peticiones OCSP* con el estado del *Certificado* por el que se consulta.
- *OID (Object Identifier)*: valor, de naturaleza jerárquica y comprensivo de una secuencia de componentes variables aunque siempre constituidos por enteros no negativos separados por un punto, que pueden ser asignados a objetos registrados y que tienen la propiedad de ser únicos entre el resto de OID.
- *Petición OCSP:* petición de consulta de estado de un *Certificado* a *OCSP Responder* siguiendo el protocolo *OCSP*.
- *PIN*: (*Personal Identification Number)* número específico sólo conocido por la persona que tiene que acceder a un recurso que se encuentra protegido por este mecanismo.
- *Prestador de Servicios de Certificación*: es aquella persona física o jurídica que, de conformidad con la legislación sobre *Firma electrónica* expide *Certificados electrónicos*, pudiendo prestar además otros servicios en relación con la *Firma electrónica*. En la presente *Declaración de Prácticas de Certificación*, se corresponderá con las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT.

- *Política de Certificación:* documento que completa la *Declaración de Prácticas de Certificación*, estableciendo las condiciones de uso y los procedimientos seguidos por ANCERT para emitir *Certificados*.
- *Póliza:* a efectos de la presente *Declaración de Prácticas de Certificación* se entenderá por la *Póliza* el documento notarial que el Notario autoriza ante el *Suscriptor* de un *Certificado* que documenta la intervención notarial como *Autoridad de Registro*, así como su intervención en el caso de revocación del mismo.
- *PKCS#10* (Certification Request Syntax Standard): estándar desarrollado por RSA Labs, y aceptado internacionalmente como estándar, que define la sintaxis de una petición de *Certificado*.
- *PUK*: (*Personal Unblocking Key)* número o clave específica sólo conocido por la persona que tiene que acceder a un recurso que se utiliza para desbloquear el acceso a dicho recurso.
- *Responsable del Fichero (o del Tratamiento del Fichero)*: persona que decide sobre la finalidad, contenido y uso del tratamiento de los *Ficheros*.
- *Responsable de Seguridad*: encargado de coordinar y controlar las medidas que impone el *Documento de seguridad* en cuanto a los *Ficheros*.
- *SHA-1*: Secure Hash Algorithm (algoritmo seguro de resumen –hash-). Desarrollado por el NIST y revisado en 1994 (*SHA-1*). El algoritmo consiste en tomar mensajes de menos de 264 bits y generar un resumen de 160 bits de longitud. La probabilidad de encontrar dos mensajes distintos que produzcan un mismo resumen es prácticamente nula. Por este motivo se usa para asegurar la *Integridad* de los documentos durante el proceso de *Firma electrónica*.
- *Sellado de Tiempo:* constatación de la fecha y hora en un documento electrónico mediante procedimientos criptográficos indelebles, basándose en las especificaciones *Request For Comments*: 3161 – *"Internet X.509 Public Key Infrastructure Time–Stamp Protocol (TSP)",* que logra datar el documento de forma objetiva.
- *Solicitante*: persona física que previa identificación, solicita la emisión de un *Certificado*.
- *Suscriptor (o Subject)*: el titular o firmante del *Certificado*. La persona cuya identidad personal queda vinculada mediatamente a los datos firmados electrónicamente, a través de una C*lave Pública* certificada por el *Prestador de Servicios de Certificación*. El concepto de *Suscriptor*, será referido en los *Certificados* y en las aplicaciones informáticas relacionadas con su emisión como *Subject*, por estrictas razones de estandarización internacional.
- *Tarjeta criptográfica*: tarjeta utilizada por el *Suscriptor* para almacenar claves privadas de firma y descifrado, para generar firmas electrónicas y descifrar mensajes de datos. Tiene la consideración de *Dispositivo seguro de creación de Firma* de acuerdo con la Ley y permite la generación de *Firma electrónica reconocida*.
- *Terceros que confían en Certificados:* aquellas personas que depositan su confianza en un *Certificado* de ANCERT, comprobando la validez y vigencia del *Certificado* según lo descrito en esta *Declaración de Prácticas de Certificación*
- *UIT (Unión Internacional de Telecomunicaciones)*: organización internacional del sistema de las Naciones Unidas en la cual los gobiernos y el sector privado coordinan los servicios y redes mundiales de telecomunicaciones.
- *X.500*: estándar desarrollado por la UIT que define las recomendaciones del directorio. Se corresponde con el estándar ISO/IEC 9594-1: 1993. Da lugar a

la serie de recomendaciones siguientes: X.501, X.509, X.511, X.518, X.519, X.520, X.521 y X.525.

- *X*.509: estándar desarrollado por la UIT, que define el formato electrónico básico para *Certificados electrónicos*.

1.8.2 Acrónimos

ANCERT	Agencia Notarial de Certificación, SL Unipersonal
CA	*Autoridad de Certificación*
CGN	Consejo General del Notariado
CP's	*Políticas de Certificación*
CPS	Declaración de Prácticas de Certificación
CRL	Lista de Revocación de *Certificados*
FQDN	Fully Qualified Domain Name
ETSI	Instituto Europeo de Estándares de Telecomunicaciones
FERN	*Firma electrónica reconocida* Notarial
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union-Telecom (UIT-Unión Internacional de telecomunicaciones)
PKI	Public Key Infrastructure (Infraestructura de Clave Pública)
PSC	Prestador de Servicios de Certificación
RA	*Autoridad de Registro*
RFC	Request For Comments
OCSP	Online Certificate Status Protocol
SSL	Secure Socket Layer

2 PUBLICACIÓN Y DIRECTORIO DE *CERTIFICADOS*

2.1. Directorio de Certificados

Las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT disponen de un *Directorio de Certificados* el cual es operativo durante las 24 horas de los 7 días de la semana. En caso de que se interrumpiera dicho servicio por causa de fuerza mayor, y por tanto ajena a dichas *Autoridades de Certificación*, el servicio se restablecerá en el estrictamente menor tiempo posible.

2.2. Publicación

Las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT permiten consultar libremente el *Directorio de Certificados* durante las 24 horas de los 7 días de la semana en la dirección http://www.ancert.com. En este *Directorio de Certificados* se podrá consultar los *Certificados* emitidos por ANCERT, y su vigencia. Asimismo se publicarán junto al *Directorio de Certificados* las *Listas de Certificados Revocados*, la

presente *Declaración de Prácticas de Certificación*, las *Políticas de Certificación* y los *Certificados Raíz* de las Autoridades pertenecientes a ANCERT.

2.3. Frecuencia de actualizaciones

La información de las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT se publicará cuando exista una actualización disponible.

2.4. Control de Acceso al Directorio de Certificados

Las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT no limitan el acceso de lectura a las informaciones establecidas en el punto 2 de este documento, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o eliminar información registrada, a fin de proteger la integridad y autenticidad de la misma. ANCERT utiliza sistemas fiables para el registro de *Certificados*, pudiendo únicamente personas autorizadas hacer modificaciones.

3 IDENTIFICACIÓN Y AUTENTICACIÓN

Las condiciones establecidas por ANCERT referentes a la identificación y autenticación de los *Solicitantes y/o Suscriptores* de *Certificados* se desarrollan para cada tipo de *Certificado* a través de las correspondientes *Políticas de Certificación.*

4 REQUISITOS OPERATIVOS DEL CICLO DE VIDA DE LOS *CERTIFICADOS*

La emisión de *Certificados* supone la generación de *Documentos electrónicos* que acreditan la identidad y, en su caso, otras cualidades o facultades del *Suscriptor.* Todos los *Certificados*, para ser tales, y con el fin de evitar su alteración o falsificación, deberán contener la *Firma electrónica reconocida* de los mismos, generada por las *Autoridades de Certificación* pertenecientes a la jerarquía de ANCERT con sus *Datos de creación de Firma* en su calidad de *Prestador de Servicios de Certificación*.

En función del tipo de *Certificado* solicitado (véase punto 1.4) variarán los procedimientos referentes al ciclo de vida de cada *Certificado.*

En este apartado se establecen las fases comunes del ciclo de vida de todos los *Certificados*, que se complementarán según cada caso, con la *Política de Certificación* que corresponda en cada caso.

4.1. Presolicitud

El trámite de presolicitud se especificará en las *Políticas de Certificación* que proceda.

4.2. Solicitud

La fase de solicitud del *Certificado* comprende con carácter general la personación ante la *Autoridad de Registro* correspondiente para la comprobación y confirmación de la identidad personal del *Solicitante*, así como la aportación de la documentación que corresponda, la cumplimentación de formularios, y suscripción de los *Contratos* que se establezcan. Todo ello se determina en las distintas *Políticas de Certificación.*

4.3. Emisión de Certificados

Los trámites comprendidos en el procedimiento de emisión del *Certificado* pueden a su vez ser distintos en función del *Certificado* solicitado. Cada uno de estos procedimientos se especifica en las *Políticas de Certificación.*

4.4. Archivo de los Datos de verificación de Firma

Los *Datos de verificación de Firma* de los *Suscriptores* permanecerán archivados por si fuera necesaria su recuperación, en archivos y soportes seguros tanto física como lógicamente, durante el período legalmente establecido de quince (15) años.

4.5. Aceptación de Certificados

La aceptación de los *Certificados* por parte del *Suscriptor* se entenderá producida desde el momento de su emisión y entrega al *Suscriptor* por ANCERT y firma de la correspondiente *Póliza*.

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 ANCERT, el *Suscriptor* del mismo declara:

a) Que toda la información entregada durante el procedimiento de solicitud del *Certificado* es verdadera.

b) Que el *Certificado* será usado exclusivamente para fines legales y autorizados por ANCERT de acuerdo a la presente *Declaración de Prácticas de Certificación* y siempre dentro del ámbito determinado en cada *Política de Certificación*.

c) 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 ANCERT 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*.

ANCERT 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.

4.6. Vigencia de los Certificados

4.6.1 Caducidad

Todos los *Certificados* emitidos por ANCERT tendrán validez, desde la emisión del *Certificado*, durante un período de tres (3) años. Fuera de este periodo de validez los *Certificado*s se considerarán inválidos para cualquier tipo de operación cesando de esta manera los servicios de certificación ofrecidos por el *PSC*, siendo necesaria la emisión de uno nuevo en caso de que el *Suscriptor* desee seguir utilizando los servicios de ANCERT.

4.6.2 Extinción

Los *Certificados* emitidos por ANCERT, exceptuando los *Certificados raíz*, se extinguen en los siguientes casos:

a) Terminación del período de validez del *Certificado* dependiendo de la *Política de Certificación* aplicable.

b) Cese en la actividad como *Prestador de Servicios de Certificación* de ANCERT, salvo que, previo consentimiento expreso del *Suscriptor*, los *Certificados* expedidos por ANCERT hayan sido transferidos a otro *Prestador de Servicios de Certificación*.

c) Revocación o Suspensión del *Certificado* por cualquiera de las causas previstas en la presente *Declaración de Prácticas de Certificación.*

d) Resolución judicial o administrativa que así lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del *Suscriptor;* de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del *Suscriptor* o de su representado; terminación o modificación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los *Datos de creación de Firma* que estén reflejadas en los *Certificados* expedidos a una persona jurídica.

4.6.3 Revocación de *Certificado*s

La solicitud de revocación de los *Certificado*s podrá efectuarse durante el período de validez que consta en el *Certificado*.

4.6.3.1 Causas de revocación

Las causas de revocación de los *Certificado*s de ANCERT son las siguientes:

a) la solicitud del *Suscriptor*, su representante, la persona física o jurídica representada por el *Suscriptor*, un tercero debidamente autorizado, o la persona física solicitante de un *Certificado* electrónico de persona jurídica.

Se deberá efectuar siempre dicha solicitud en los siguientes casos:

- Pérdida del soporte de los *Datos de creación de Firma*.
- Utilización indebida por un tercero de los *Datos de creación de Firma* del *Suscriptor*.
- Violación o puesta en peligro del secreto de los *Datos de creación de Firma* del *Suscriptor.*

b) la resolución del *Contrato* de prestación de servicios de certificación en los supuestos de que *Suscriptor*, su representante, la persona física o jurídica representada por el *Suscriptor* o un tercero debidamente autorizado incurra en los siguientes supuestos:

- Alteración de los datos aportados por el *Solicitante* para la obtención del *Certificado* o modificación de las circunstancias verificadas para la expedición del *Certificado,* como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.
- Utilizar los datos de creación de firma cuando haya expirado el período de validez del *Certificado* electrónico o ANCERT le notifique la extinción o suspensión de su vigencia.
- Superar los límites que figuren en el *Certificado electrónico* en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al *Suscriptor* por el prestador de servicios de certificación.
- No haber proporcionado a ANCERT información veraz, completa y exacta sobre los datos que deban constar en el *Certificado electrónico* o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.
- La falta de comunicación a ANCERT, sin demora, de cualquier modificación de las circunstancias reflejadas en el *Certificado electrónico*.
- Negligencia en la conservación de sus *Datos de creación de Firma*, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
- No solicitar la suspensión o revocación del *Certificado* en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- La suspensión del *Certificado* por un periodo superior a 60 días en las condiciones que se establezcan en presente *CPS* o en las correspondientes *Políticas de Certificación.*
- Contravenir cualquier obligación establecida en la presente *CPS* o en las correspondientes *Políticas de Certificación.*

4.6.3.2 Procedimiento para la revocación de Certificados

El legítimo solicitante de la revocación deberá efectuar las actuaciones pertinentes de conformidad con el procedimiento específico que corresponda según la *Política de Certificación* establecida para su tipo de *Certificado*.

- Bases del procedimiento de revocación para *Certificado*s expedidos por **ANCERT *Certificado*s Notariales**

Sin perjuicio de lo que establezca la Política de Certificación de cada *Certificado*, deberá seguirse en todo caso lo siguiente:

- La revocación voluntaria del *Suscriptor* se podrá efectuar ante Notario, que autorizará una *Póliza* de revocación de *Certificado*.
- No cabe en ningún caso la revocación mediante envío de correo electrónico, ni ningún otro medio a disposición del *Suscriptor* salvo lo exceptuado en el punto siguiente.
- El *Suscriptor* del *Certificado* podrá instar su revocación mediante envío de un correo electrónico firmado electrónicamente con el *Certificado* a revocar, dirigido a ANCERT, a la dirección de correo electrónico *revocacion@ancert.com*. La revocación se llevará a cabo inmediatamente después de su recepción.
- En el caso de haberse producido una previa suspensión de un *Certificado*, y transcurrido un tiempo superior a 60 días sin que el *Suscriptor* haya solicitado el levantamiento de la suspensión, ANCERT revocará el *Certificado*.

- Bases del procedimiento de revocación para *Certificado*s expedidos por **ANCERT *Certificado*s Redes Privadas**

Se establecerá en la *Política de Certificación* correspondiente.

- Bases del procedimiento de revocación para *Certificado*s expedidos por **ANCERT Corporaciones de Derecho Público:**

Se establecerá en la *Política de Certificación* correspondiente.

- Bases del procedimiento de revocación para *Certificado*s expedidos por **ANCERT *Certificado*s CGN:**

Se establecerá en la *Política de Certificación* correspondiente.

4.6.3.3 Efectos de la revocación

Los efectos de la revocación del *Certificado*, esto es, la extinción de su vigencia, surtirán desde la fecha en que ANCERT tenga conocimiento efectivo de la revocación

por su legítimo solicitante o haya resuelto el contrato con el *Suscriptor*, y así lo haga constar en el *Directorio de Certificados* y en la *Lista de Revocación de Certificados*.

4.6.4 Suspensión de los Certificados

La solicitud de suspensión de los *Certificado*s podrá realizarse durante el período de validez de los mismos dependiendo de cada *Política de Certificación*.

4.6.4.1 Causas de la suspensión

Son causas de suspensión de la vigencia de los *Certificado*s:

a) Solicitud del *Suscriptor*, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un *Certificado electrónico* de persona jurídica.
b) 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. En este caso ANCERT, suspenderá la vigencia del *Certificado* por el plazo que dure el procedimiento y transcurrido el mismo se procederá a la reactivación del mismo.
c) La existencia de dudas fundadas acerca de la concurrencia de las causas de revocación de la vigencia de los *Certificado*s contempladas en el punto 4.6.3.1 de esta *CPS*.

4.6.4.2 Efectos de la suspensión

Los efectos de la suspensión del *Certificado* son la extinción de su vigencia que surtirá efectos desde la fecha en que ANCERT tenga conocimiento efectivo de cualquiera de las causas de suspensión, y así lo haga constar en el *Directorio de Certificados* y en la *Lista de Revocación de Certificados.*

4.6.4.3 Procedimiento para la suspensión de Certificados

El legítimo solicitante de la suspensión deberá seguir los trámites particulares que se establezcan en cada *Política de Certificación* establecida para su tipo de *Certificado*.

Sin perjuicio de lo anterior, el *Solicitante* que voluntariamente solicite la suspensión deberá telefonear al teléfono 902 348 347 del Centro de Atención a Usuarios de ANCERT. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante de la suspensión será sometida a grabación y almacenada en un dispositivo seguro. El solicitante de la suspensión deberá responder con la contraseña o secreto compartido indicado por el mismo durante el proceso de solicitud de *Certificado*. En caso de que la respuesta coincida con dicha contraseña el operador procederá a suspender el *Certificado*.

4.6.4.4 Procedimiento para levantar la suspensión de Certificados

El legítimo solicitante de la suspensión podrá proceder a levantar la suspensión de los *Certificado*s, según la *Política de Certificación* establecida para su tipo de *Certificado*.

4.6.5 Emisión y publicación de Certificados Revocados

En el *Directorio de Certificados* constará de manera inmediata la revocación efectuada por el legítimo solicitante y en la *CRL* en el modo que se establezca en la correspondiente *Política de Certificación.*

4.6.6 Procedimientos de consulta del estado de los *Certificado*s

El *Suscriptor* del *Certificado* tendrá acceso al *Directorio de Certificados* y a las *Listas de Revocación de Certificados* a través de la Web www.ancert.com en el modo que se establezca en la correspondiente *Política de Certificación.*

4.6.7 Obligación de consulta de los *Certificado*s Revocados

Los *Terceros que confían en Certificado*s han de comprobar, obligatoriamente, el estado de aquellos *Certificado*s en los que se quiere confiar en las condiciones establecidas en la *Política de Certificación* correspondiente. Se comprueba el estado de los *Certificado*s consultando el *Directorio de Certificados* o bien la *CRL* más reciente emitida por la *Autoridad de Certificación* que emitió el *Certificado* en el que se quiere confiar.

4.6.8 Disponibilidad de servicios de comprobación del estado de los *Certificado*s

Los *Terceros que confían en Certificado*s pueden consultar el *Directorio de Certificados* de ANCERT, a través de la *Web* www.ancert.com, que está disponible las 24 horas de los 7 días de la semana.

4.7. Renovación de Certificados

No podrá solicitarse la renovación de los *Certificado*s emitidos por ANCERT. En caso de caducidad del *Certificado* el interesado que lo desee deberá nuevamente comparecer en la forma anteriormente vista para obtener la emisión de un nuevo *Certificado*.

4.8. Notificación de la extinción o suspensión de Certificados

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 **ANCERT** 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.

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

4.9. Cese de la Actividad de ANCERT como Prestador de Servicios de Certificación

ANCERT comunicará, en su caso, el cese de su actividad, a los *Suscriptores* que utilicen los *Certificados electrónicos* que haya expedido así como a los *Solicitantes* de *Certificados* expedidos a favor de personas jurídicas; 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 el *PSC* publicará en el Web del servicio de certificación y en un periódico de ámbito nacional esta circunstancia con una antelación mínima de dos meses.

ANCERT 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 él.

ANCERT 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.

5 Controles de Seguridad

ANCERT ha implantado controles de seguridad y auditorias que se desarrollan en el presente punto.

5.1. Controles de seguridad física, de procedimientos y del personal

En este apartado se describen los controles de seguridad física, de los procedimientos y del personal implantados por ANCERT para la realización de sus actividades.

5.1.1 Controles de seguridad física

ANCERT ha establecido controles de seguridad física con objeto de reducir el riesgo de accesos no autorizados o de daños a los recursos informáticos.

5.1.1.1 Situación de las instalaciones

El edificio donde se encuentra ubicado el Centro de Proceso de Datos (CPD) de ANCERT dispone de medidas de seguridad de control de acceso al edificio, dotado de sistemas de video vigilancia.

El Centro de Proceso de Datos (CPD) de ANCERT ha sido construido y situado en un local sin riesgo de inundaciones, sin ventanas al exterior del edificio, controlado su acceso al interior con tarjeta de identificación y PIN de acceso, disponiendo de sistemas de protección y prevención de incendios.

5.1.1.2 Acceso físico

El acceso físico a las instalaciones donde ANCERT realiza su actividad como *PSC* está restringido solamente a personal autorizado.

Existen varios perímetros de seguridad para evitar el acceso de personal no autorizado así como para controlar y registrar el acceso de personal autorizado.

5.1.1.3 Electricidad y aire acondicionado

El CPD cuenta con sistemas de aire acondicionado en funcionamiento simultáneo y redundante que aseguran la estabilidad de la temperatura de en la sala necesaria para el funcionamiento fiable y óptimo de los equipos.

El suministro eléctrico está asegurado por varios niveles de equipamiento.

5.1.1.4 Exposiciones al agua

ANCERT toma las medidas necesarias para evitar la exposición al agua de sus medios materiales.

5.1.1.5 Prevención y protección contra incendios

Las instalaciones disponen de las medidas adecuadas contra incendios de los equipos informáticos así como del cableado del *PSC*.

5.1.1.6 Almacenamiento de soportes

ANCERT, como *Prestador de Servicios de Certificación*, establece los procedimientos necesarios de almacenamiento para disponer de las copias de respaldo de la información.

5.1.1.7 Política eliminación de residuos

El personal de ANCERT dispone de los instrumentos necesarios para la destrucción de información u otros residuos.

5.1.1.8 Copias de Seguridad fuera de las instalaciones

ANCERT dispone de un servicio de almacenamiento de las copias de seguridad de la información fuera de sus instalaciones.

5.1.2 Controles de seguridad de procedimientos

ANCERT garantiza que los procedimientos de operaciones se lleven a cabo de acuerdo con esta *Declaración de Prácticas de Certificación*.

5.1.3 Controles de seguridad del Personal

Cada puesto de trabajo tiene asignada su grado de responsabilidad en el cumplimiento de las medidas de seguridad implantadas por ANCERT.

5.1.3.1 Conocimientos, calificación, experiencia y requerimientos acreditativos

Los conocimientos, calificación, experiencia y requerimientos acreditativos del personal de la infraestructura de ANCERT aseguran su capacidad en el cumplimiento de sus obligaciones.

5.1.3.2 Procedimiento disciplinario

El personal de ANCERT está obligado a cumplir lo siguiente:

- Utilizar los medios materiales de ANCERT 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 ANCERT.
- 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 ANCERT 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 ANCERT, 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 ANCERT 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 ANCERT 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 ANCERT 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 ANCERT, 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 efectuarán previa aprobación por el Departamento de Seguridad, de acuerdo con el procedimiento establecido en la normativa aplicable.

ANCERT podrá eliminar de su sistema informático cualquier material que considere ofensivo o potencialmente ilegal.

5.1.3.3 Actividades no autorizadas

En materia de seguridad, son actividades no autorizadas para los empleados de ANCERT:

- Compartir o facilitar los identificadores de usuario y/o la clave de acceso facilitados por ANCERT 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 ANCERT.
- Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos *electrónicos* de ANCERT o de terceros.
- Obstaculizar voluntariamente el acceso de otros empleados a la red mediante el consumo masivo de los recursos informáticos y telemáticos de ANCERT, 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 ANCERT 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 ANCERT 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 ANCERT.
- Instalar copias ilegales de cualquier programa, incluidas las estandarizadas.
- Borrar cualquiera de los programas instalados legalmente.
- Utilizar los recursos telemáticos de ANCERT incluida la red Internet, para actividades que no estén relacionadas con el lugar de trabajo del empleado.
- Introducir en la red corporativa de ANCERT 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 ANCERT.
- 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 ANCERT.
- Cualquier otra actividad expresamente prohibida en la política de Seguridad de ANCERT 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 ANCERT, 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.

5.2. Registro de Eventos

5.2.1 Tipos de eventos registrados

ANCERT registra y almacena todas las acciones llevadas a cabo sobre los sistemas de Certificación que incluyen entre los más relevantes: la gestión del ciclo de vida de los *Certificados*, intentos de acceso al los sistemas de la Certificación, publicación de información en el *Directorio de Certificados* y peticiones realizadas al sistema de Certificación y al *Directorio de Certificados.*

5.2.2 Auditoria de registros de eventos

Todos los registros de eventos son auditables exclusivamente por personal autorizado por ANCERT.

Se han implantado sistemas que impiden la modificación o eliminación de los registros de eventos.

5.2.3 Copia de Seguridad de los registros de eventos

ANCERT efectúa copias de seguridad de todos los registros de eventos.

Los sistemas informáticos utilizados para realizar las copias de seguridad de los registros de eventos son propios de ANCERT almacenándose la información en soportes removibles. Dichos soportes son custodiados por una empresa de seguridad contratada a tales efectos.

5.3. Almacenamiento de archivos

5.3.1 Archivos almacenados

ANCERT registra y almacena los siguientes archivos relacionados con la actividad de *Prestador de Servicios de Certificación*:

- Emisión, revocación y suspensión de *Certificados*
- Solicitudes de emisión, revocación y suspensión de *Certificados*

- Eventos del sistema de Certificación
- Documentación relacionada con la actividad de *Prestador de Servicios de Certificación*
- Generación de claves privadas para la creación de *Certificados Raíz* y *Certificados* Subordinados.
- *Listas de Revocación de Certificados*.
- El *Directorio de Certificados*.

5.3.2 Protección de los archivos

La información almacenada por ANCERT se almacena como mínimo durante un periodo de 15 años desde su generación o recepción.

ANCERT ha establecido procedimientos lógicos y físicos para proteger los archivos relacionados con la actividad de *Prestador de Servicios de Certificación*:

- Protección contra accesos no autorizados.
- Protección contra modificación, alteración, pérdida o eliminación de información.

5.3.3 Copia de Seguridad de los archivos

ANCERT efectúa copias de seguridad de todos los archivos relacionados con la actividad de *Prestador de Servicios de Certificación*.

Los sistemas informáticos utilizados para realizar las copias de seguridad de los archivos son propios de ANCERT almacenándose la información en soportes removibles. Dichos soportes son custodiados por una empresa de seguridad contratada a tales efectos.

5.3.4 Obtención y verificación de archivos

El acceso a archivos está limitado al personal autorizado por ANCERT.

5.4. Controles de seguridad técnica

5.4.1 Generación e instalación del par de claves

5.4.1.1 Generación e instalación de las Claves del Prestador de Servicios de Certificación

Por motivos de seguridad y calidad las claves que ANCERT necesita para el desarrollo de su actividad como *Prestador de Servicios de Certificación* se generarán en módulos de *hardware* criptográficos con certificación FIPS 140-1 Nivel 3.

Las operaciones de firma de *Certificado*s y de listas de revocación son llevadas a cabo dentro del dispositivo criptográfico, lo que asegura que los *Datos de creación de Firma* del *Prestador de Servicios de Certificación* nunca se encuentran sin cifrar fuera del módulo.

Los pares de claves de los operadores y administradores de las *Autoridades de Registro* se generan siempre en tarjetas inteligentes que garantizan el grado necesario de seguridad.

5.4.1.2 Generación y instalación de Claves de usuario

Las *Claves Privadas* de las *Entidades finales* se generan en *Tarjeta Criptográfica*, dispositivos criptográficos seguros o en *software*, este último tratándose únicamente de servidores *SSL*. ANCERT no tiene acceso a las *Claves Privadas* de las *Entidades finales* en ningún estadio del ciclo de vida de las mismas.

Las *Claves Privadas* son de uso exclusivo del *Suscriptor* del *Certificado*.

ANCERT conserva la C*lave Pública* del usuario según el ordenamiento legal vigente, durante un periodo no menor de 15 años.

5.4.1.3 Distribución de la clave pública de la *Autoridad de Certificación*

Las *Claves Públicas* correspondientes a los *Certificado*s r*aíz* y *Certificado*s subordinados de ANCERT pueden ser consultados y descargados a través de la página Web de ANCERT www.ancert.com

5.4.1.4 Distribución de la clave pública de usuario

En cada *Política de Certificación* se especifica el modo en el que se le hace llegar al usuario su correspondiente la *Clave Pública*.

Las *Claves Públicas* correspondientes a los *Certificado*s de los usuarios pueden ser consultados y descargados a través de la página Web de ANCERT www.ancert.com.

5.4.1.5 Periodo de utilización de las claves de usuario

Las Claves Privadas de los Usuarios podrán utilizase durante todo el periodo de vigencia del *Certificado*.

5.4.1.6 Periodo de utilización de las claves de ANCERT

Las *Claves Privadas* de las *Autoridades de Certificación* r*aíz* de ANCERT tienen una validez de veinte (20) años.

Las *Claves Privadas* de las *Autoridades de Certificación Subordinadas* tienen una validez de diez (10) años.

5.4.1.7 Usos de los Datos de creación y de verificación de Firma del Prestador de Servicios de Certificación

Los *Datos de creación y de verificación de Firma* de las *Autoridades de Certificación* de ANCERT en su actividad como *Prestador de Servicios de Certificación* serán utilizadas única y exclusivamente para los propósitos de:

- Firma de *Certificado*s para Autoridades s*ubordinadas*.
- Firma de *Certificado*s a *Entidades finales*
- Firma de las *Listas de Revocación de Certificados*.

5.4.1.8 Usos de las claves de usuario

El uso de las *claves* de los usuarios se determinará en las distintas *Políticas de Certificación* de cada uno de los *Certificados*.

5.4.2 Protección de la clave privada

5.4.2.1 Niveles de seguridad

El nivel de seguridad de los módulos *hardware* criptográficos que se utilizan para crear y almacenar las *Claves Privadas* de las *Autoridades de Certificación* es FIPS 140-1 Nivel 3.

El nivel de certificación de seguridad de la plataforma PKI ha alcanzado el Common Criteria EAL4+.

Respecto a los datos personales se restará a lo especificado la normativa legal vigente y en concreto el RD 994/1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los *Ficheros* automatizados que contengan datos de carácter personal.

5.4.2.2 Fin del ciclo de vida de las Claves del Prestador de Servicios de Certificación

ANCERT dispondrá de todos los medios necesarios para asegurar que una vez finalizado el periodo de validez de las *Claves Privadas* del *Prestador de Servicios de Certificación*, estas claves no vuelven a ser utilizadas, procediéndose de forma inmediata a su destrucción.

5.4.3 Datos de Activación de la *Autoridad de Certificación*

En el proceso de instalación del *Módulo Criptográfico Hardware de Seguridad* se generan varias tarjetas necesarias para la activación de la *Autoridad de Certificación*, cada tarjeta tiene un PIN diferente y está en posesión de un custodio.

Para la activación de la *Autoridad de Certificación* es necesaria la intervención de varios de los custodios de las tarjetas de activación.

5.4.4 Controles de seguridad de la red

Se han establecido controles activos y pasivos de seguridad para detectar y reaccionar ante cualquier intento de agresión, manipulación o acceso no autorizado a través de las redes de acceso público y de acceso restringido de ANCERT.

6 OBLIGACIONES

6.1. Obligaciones de ANCERT previas a la expedición de Certificados reconocidos

Antes de expedir un *Certificado* ANCERT se obliga a lo siguiente:

a) Comprobar la identidad y circunstancias personales de los *Solicitantes y/o Suscriptores* de *Certificados* de acuerdo con la presente *Declaración de Prácticas de Certificación* y a las correspondientes *Políticas de Certificación.*
b) Verificar que toda la información contenida en la solicitud del *Certificado* es exacta y que incluye toda la información prescrita para un *Certificado* reconocido.
c) Asegurarse de que el *Suscriptor* de un *Certificado* está en posesión de, los *Datos de creación de Firma* correspondientes a los de *Datos de verificación de Firma* que constan en el *Certificado.*
d) Garantizar la complementariedad de los datos de creación y verificación de firma.
e) Proporcionar al *Solicitante* del *Certificado* la siguiente información mínima, que se transmitirá de forma gratuita, por escrito o por vía electrónica:

    1) Las obligaciones del *Suscriptor*, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de *Firma electrónica* que sean compatibles con los datos de firma y con el *Certificado* expedido.
    2) Los mecanismos para garantizar la fiabilidad de la *Firma electrónica* de un documento a lo largo del tiempo.
    3) El método utilizado por el prestador para comprobar la identidad del *Suscriptor* u otros datos que figuren en el *Certificado*.

4) Las condiciones precisas de utilización del *Certificado*, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.
5) Las demás informaciones contenidas en la *CPS*.

6.2. Obligaciones de ANCERT simultáneas o posteriores a la expedición de Certificados reconocidos.

Simultánea o posteriormente a la expedición de los *Certificado*s, ANCERT se obliga a:

a) No almacenar ni copiar los *Datos de Creación de Firma* de la persona a la que hayan prestado sus servicios.
b) Mantener un *Directorio* actualizado de *Certificado*s en el que se indicarán los *Certificado*s expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.
c) Demostrar la fiabilidad necesaria para prestar servicios de certificación.
d) Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un *Certificado* o se extinguió o suspendió su vigencia.
e) Emplear personal cualificado y con la experiencia necesaria para la prestación de los servicios ofrecidos.
f) Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica, y en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
g) Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un *Certificado* reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.
h) Utilizar sistemas fiables para almacenar *Certificado*s *reconocidos* que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el *Suscriptor* haya indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.
i) Revocar el *Certificado* y a publicar ese hecho en su CRL de un modo inmediato, una vez recibida la correspondiente solicitud de revocación. La solicitud de revocación deberá ser cursada en la forma prevenida en la *Declaración de Prácticas Certificación* y consiguientes *Políticas de Certificación.*
j) Poner a disposición de los usuarios los medios necesarios para verificar la autenticidad de los *Certificado*s emitidos.
k) Facilitar el acceso por medios telemáticos a esta *CPS*, a las *Políticas de Certificación* y a las versiones actualizadas de las mismas.
l) Cumplir todas las previsiones de la normativa sobre protección de datos de carácter personal.
m) Emitir los *Certificado*s solicitados ajustándose a las normas y procedimientos establecidos en la presente *Declaración de Prácticas de Certificación* y consiguientes *Políticas de Certificación*.

n) Cumplir todas aquellas obligaciones impuestas por la presente *Declaración de Prácticas Certificación*, las *Políticas de Certificación* y por la normativa vigente en materia de *Firma electrónica* y prestación de servicios de certificación.

6.2.1 Obligaciones de la *Autoridad de Registro*

ANCERT podrá delegar a una *Autoridad de Registro*, entre otras funciones de la actividad de PSC, las funciones de identificación, autenticación y registro de *Solicitantes, Suscriptores y Representados* de *Certificados*, en cuyo caso quedará obligada al cumplimiento de las mismas obligaciones y en iguales condiciones que ANCERT. Por ello, la *Autoridad de Registro* actuará en nombre propio aunque por cuenta de ANCERT.

Las obligaciones de la *Autoridad de Registro* se establecen en las correspondientes *Políticas de Certificación* de las que los suscriptores podrán tomar conocimiento a través de la Web de ANCERT.

En todo caso la *Autoridad de Registro*, deberá aplicar los procedimientos establecidos por ANCERT en la presente *Declaración de Prácticas de Certificación* y en las *Políticas de Certificación*, en el desempeño de sus funciones de gestión, emisión, renovación y revocación de *Certificados.*

6.2.2 Obligaciones del Suscriptor

Son obligaciones del *Suscriptor*:

1. Abonar las tarifas que se devenguen por los servicios de certificación que soliciten.
2. Solicitar y recibir el *Certificado* siguiendo los procedimientos descritos en la presente *Declaración de Prácticas de Certificación* y en las correspondientes *Políticas de Certificación.*
3. Mantener el compromiso para todo el periodo de vigencia del *Certificado*, de que toda la información contenida en el *Certificado* es cierta y se compromete a notificar cualquier modificación, actualización o inexactitud de la misma.
4. Utilizar el *Certificado* exclusivamente dentro de los límites especificados en el momento de su concesión.
5. No utilizar el *Certificado* desde el momento que solicita su revocación o fuera del periodo de validez.
6. Proteger y custodiar de forma diligente el *Certificado*, las claves, el soporte de las mismas, y cualquier otro *Dato de Creación o Verificación de Firma,* tomando las precauciones razonables para evitar su perdida, revelación, modificación o uso no autorizado.
7. No ceder los *Datos de creación de Firma*, que son intransferibles, pudiendo ser únicamente utilizados por la persona física o jurídica titular del *Certificado*.
8. Notificar de forma inmediata la pérdida o divulgación de la *Clave Privada*, o cualquier situación que pueda afectar a la validez del *Certificado*, o su confidencialidad, solicitando su revocación en forma inmediata, en cuanto se tenga conocimiento de ello, indistintamente a cualquier *Autoridad de Registro*.
9. Conocer y cumplir con todas aquellas obligaciones impuestas en esta Declaración de Prácticas de Certificación y en las *Políticas de Certificación*.

10. Verificar con carácter previo a confiar en los *Certificado*s, la *Firma electrónica reconocida* del Prestador de Servicios de Certificación emisor del *Certificado*.
11. Dar su consentimiento para la publicación en el *Directorio de Certificado*s de sus datos personales contenidos en el *Certificado*.

6.2.3 Obligaciones del *Representado*

Sin perjuicio de las obligaciones que correspondan en cada caso al suscriptor del *Certificado*, el *Representado* deberá solicitar a ANCERT la revocación del *Certificado* tan pronto revoque el poder otorgado al representante o resulten extinguidas por cualquier otra causa las facultades de representación.

6.2.4 Obligaciones de los Terceros que confían en los *Certificado*s

Son obligaciones de los *Terceros que confían en Certificados* emitidos por ANCERT:

1. Verificar, previamente a confiar en *Certificado*s emitidos por ANCERT, la *Firma electrónica reconocida* del *Prestador de Servicios de* Certificación emisor del *Certificado*.
2. Verificar el estado de los *Certificado*s en la cadena de certificación, mediante consulta a las *Listas de Revocación de Certificados* o consultando el *Directorio de Certificados* de ANCERT.
3. Comprobar y tener en cuenta las restricciones que figuren en los *Certificados* en cuanto a los posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
4. Notificar a ANCERT o a cualquier *Autoridad de Registro*, cualquier anomalía relativa a un *Certificado* y que pueda ser considerada como causa de revocación del mismo.

7 RESPONSABILIDADES

7.1. Responsabilidades de ANCERT

ANCERT responderá en el caso de incumplimiento de todas aquellas obligaciones impuestas por la presente *Declaración de Prácticas de Certificación*, la *Ley de Firma electrónica* y la normativa existente en materia de prestación de servicios de certificación, excepto respecto de los daños y perjuicios causados por las siguientes causas:

1. El incumplimiento de las obligaciones que corresponden a cada *Suscriptor* de los *Certificados*.

2. La utilización de los *Certificados* y/o claves certificadas por ellos, para usos no permitidos en el *Certificado*, o por su utilización fuera del periodo de vigencia del *Certificado*.

3. La pérdida, divulgación o compromiso de la clave privada del *Suscriptor*; o por el uso incorrecto de los soportes que contienen los *Certificados* y las claves.

4. El contenido de los documentos firmados digitalmente con una firma basada en un *Certificado* emitido por él.

5. Caso fortuito o fuerza mayor tales como los desastres naturales o la guerra, o los cortes en el suministro electrónico o en el funcionamiento defectuoso de los equipos informáticos utilizados por el *Suscriptor* o por los *Terceros que confían en Certificados*.

Sin perjuicio de lo anterior, ANCERT 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 *Prestador de Servicios de Certificación* y en la Ley 59/2003 y su normativa de aplicación.

7.2. Responsabilidad de la Autoridad de Registro

La responsabilidad por su actuación dolosa o culposa de la *Autoridad de Registro* se establecerá en cada una de las *Políticas de Certificación* de los *Certificado*s.

7.3. Responsabilidad del Solicitante

El *Solicitante* responderá por los daños causados como consecuencia de la no veracidad o exactitud de la información aportada durante el proceso de solicitud del *Certificado*.

Asimismo la custodia de los Datos de Creación de Firma asociados a cada *Certificado* electrónico emitido por ANCERT cuyo Suscriptor sea una persona jurídica, será responsabilidad de la persona física Solicitante/Custodio cuya identificación se haya incluido en el *Certificado*.

7.4. Responsabilidad del Suscriptor

El *Suscriptor* responderá en caso de incumplimiento de sus obligaciones, y en todo caso, del uso indebido del *Certificado*, o de la no veracidad o exactitud de la información aportada en todo momento a ANCERT o terceros.

7.5. Responsabilidad de los Usuarios de Certificados

Los Usuarios de *Certificados* emitidos por ANCERT son responsables de cumplir la presente *Declaración de Prácticas de Certificación* y las correspondientes *Políticas de Certificación.*

Los Usuarios de *Certificado*s emitidos por ANCERT son responsables de actuar de forma diligente verificando en todo caso las firmas electrónicas reconocidas de los documentos *electrónicos* y los *Certificados* emitidos por ANCERT.

En ningún caso podrá presumirse la autenticidad de los documentos *electrónicos* o los *Certificado*s.

8 Protección de Datos de Carácter Personal

8.1. Normativa aplicable

La normativa aplicable para la redacción del Documento de Seguridad es la siguiente:

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de esos datos.
- Directiva 97/66/CE del Parlamento Europeo y del Consejo, de 15 de diciembre de 1997, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las telecomunicaciones.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
- Real Decreto 994 / 1999, de 11 de junio, por el que se aprueba el Reglamento de medidas de seguridad de los *Ficheros* automatizados que contengan datos de carácter personal.

8.2. Ámbito de aplicación de la Protección de Datos

ANCERT protegerá 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 Reglamento de medidas de seguridad aprobado por el Real Decreto 994/1999, de 6 de junio (*RD 994/1999*) y demás normativa de desarrollo. Dichos *Ficheros* serán de titularidad privada y su creación, modificación o supresión se notificarán al Registro General de Protección de Datos de la Agencia Española de Protección de Datos.

Para realizar su actividad de certificación las A*utoridades de Registro* accederán a dichos F*icheros*.

ANCERT tendrá la condición de Responsable del Fichero en tanto que decidirá sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal y las *Autoridades de Registro* se considerarán Encargadas del Tratamiento, las cuales

deberán utilizar los datos contenidos en dichos *Ficheros*, única y exclusivamente para los fines que figuran en su *Declaración de Prácticas de Certificación.*

Las *Autoridades 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 a que está obligado según el *RD 994/1999*.
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. Las medidas de seguridad mencionadas son las determinadas en el *RD 994/1999*.
6. A remitir a ANCERT 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 ANCERT, 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 ANCERT 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 ANCERT, salvo aquellos datos que la legislación obliga a conservarlos por un mínimo de 15 años.

Las *Autoridades de Registro* verificarán 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.

ANCERT 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. ANCERT 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 ANCERT 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 *Certificado*s 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 *Directorio de Cerificados* que consta en la página Web www.ancert.com exclusivamente para la finalidad de permitir la consulta de los *Certificado*s emitidos por ANCERT y la vigencia de los mismos, así en el *Directorio de Certificados* y las *Listas de Certificados Revocados* para consultar los *Certificados* revocados por ANCERT.

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 el punto 1.7.1

8.3. Documento de seguridad

8.3.1 Objetivo del Documento de Seguridad

Mediante el presente documento ANCERT 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, ANCERT, directamente o a través de las *Autoridades 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 994/1999, ANCERT 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 ANCERT, para evitar su alteración, pérdida, tratamiento o acceso no autorizado y ser utilizados para una finalidad legítima.

Con el *Documento de Seguridad,* ANCERT 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 ANCERT 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 994/1999* 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.

8.3.2 Funciones y obligaciones del personal

El personal de ANCERT como usuarios que tratan los *Ficheros* conoce y cumple sus funciones y obligaciones establecidas en el *Documento de Seguridad* de ANCERT. 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 encargará de que los datos de carácter personal que se incorporen al sistema de información de ANCERT estén debidamente legitimados.
2. Supervisará que la solicitud de los datos cumple con los siguientes principios:

    a) Principio de consentimiento: El tratamiento de los datos de carácter personal, requerirá el consentimiento expreso, preciso e inequívoco del titular.
    b) Principio de información: se deberá informar previamente al titular de los datos personales de manera expresa, precisa e inequívoca de:

        1. La existencia de un Fichero o tratamiento de datos de carácter personal.
        2. La identidad y dirección del Responsable del Fichero.
        3. La finalidad de la recogida.
        4. Los destinatarios de la información.
        5. Del carácter obligatorio o facultativo de su respuesta a las preguntas que le sean planteadas.
        6. Las consecuencias de la obtención de los datos personales y de las consecuencias de la negativa a suministrarlos.
        7. 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 ANCERT es responsable.

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

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

- Dentro del ámbito tecnológico sus funciones son:

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

1. La identificación y autenticación de los usuarios.
2. Del procedimiento de respaldo y recuperación de la Información personal.
3. La organización de los soportes automatizados.
4. Realizar auditorias o revisiones.
5. Controlar las incidencias.

- Dentro del ámbito físico sus funciones son:

a) 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 encargará de:

1. La identificación y autenticación de los usuarios.
2. Del procedimiento de respaldo y recuperación de la Información personal.
3. La organización de los soportes físicos.
4. Realizar auditorias o revisiones.
5. 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:

- Planificar, ejecutar y controlar las Medidas de Seguridad de los dispositivos de hardware, software a los distintos aplicativos y comunicaciones, por ello se encargará de:

    1. La identificación y autenticación de los Usuarios.
    2. Del procedimiento de respaldo y recuperación de la Información personal.
    3. La organización de los soportes automatizados.
    4. Realizar auditorias o revisiones.
    5. Controlar las incidencias.

8.3.3 Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en el RD 994/1999.

Este apartado recoge las medidas de seguridad de obligado cumplimiento que debe cumplir ANCERT para dar cumplimiento al artículo 8 del *RD 994/1999*.

Centros y zonas de tratamiento

ANCERT 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.

ANCERT dispone de los medios suficientes de seguridad. Ha establecido medidas físicas de control de accesos desde el exterior del edificio donde se ubica ANCERT, mediante sistemas de vídeo vigilancia, además de los medios humanos dedicados a su protección, así como controles internos de las salas e instalaciones como son los controles de accesos basado en lectores de tarjetas, detectores de intrusismo, detectores de incendios, etc.

En lo relativo a los accesos físicos interiores, en cuanto a las oficinas, existe una política de equipar con cerraduras y medidas de seguridad las puertas de acceso con lo que se habilita su función de restringir el acceso a las mismas.

ANCERT dispone de un reglamento de llaves con el fin de supervisar y controlar la asignación de llaves, y por tanto la responsabilidad sobre los accesos físicos por parte del personal autorizado.

ANCERT dispone de un inventario de usuarios que disponen de copia de las llaves antes descritas. Las copias no asignadas a ningún usuario estarán en posesión del *Responsable de Seguridad* según se determine en el reglamento de llaves. Los usuarios no pueden bajo ningún concepto realizar copias de llaves estando atribuida dicha función al *Responsable de Seguridad*.

En las llaves que se describen en el reglamento de llaves se deja constancia de un código cifrado que puede relacionarse con dicho reglamento en el que se describe a qué cerradura y acceso físico corresponde dicha llave y el número exacto de copias que existen en circulación.

Puestos de trabajo

ANCERT dispone de un inventario de puestos de trabajo correspondiente a usuarios autorizados para acceder a la información de carácter personal, que estará bajo la responsabilidad de una persona previamente autorizada.

Todos los equipos están situados y orientados de tal forma que garantizan la confidencialidad de la información de carácter personal.

Los usuarios que tengan acceso a información de carácter personal tienen una configuración fija en sus aplicaciones y sistemas operativos, que sólo puede ser modificada bajo la autorización del *Responsable de Seguridad***.**

Dispositivos de almacenamiento físico

Los soportes físicos con información de carácter personal gozan de una administración correcta. Las medidas de seguridad son adecuadas en lo que respecta al acceso, almacenándose en locales o dispositivos de almacenamiento físico cuyo acceso se encuentre debidamente restringido.

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

ANCERT 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 de personal necesarios para la creación de un *Certificado* electrónico genera *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 ANCERT 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*.

8.3.4 Estructura del *Fichero* con datos de carácter personal

La estructura del *Fichero* de datos de carácter personal utilizado por ANCERT 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
- Lugar y fecha de nacimiento
- Nacionalidad
- Empresa de trabajo
- Atributos (titulación, pertenencia a colegios profesionales, cargos públicos)

8.3.5 Procedimiento de notificación, gestión y respuesta ante las incidencias

El personal de ANCERT 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.

8.3.6 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.

8.3.7 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.

9 Propiedad Intelectual e Industrial

ANCERT es titular en exclusiva de todos los derechos, incluidos los derechos de explotación, sobre el *Directorio de Certificados* y la *Lista de Revocación de Certificados* en los términos señalados en el Texto Refundido de la Ley de Propiedad Intelectual aprobado mediante Real Decreto Legislativo 1/1996, de 12 de abril, incluido el derecho *sui generis* reconocido en el artículo 133 de la citada Ley.

Se permite el acceso al *Directorio de Certificados* y *Listas de Revocación de Certificados* estando prohibida la reproducción, comunicación pública, distribución, transformación o reordenación salvo cuando esté expresamente autorizada por ANCERT o por la Ley.

Asimismo, ANCERT es titular de todos los mismos derechos de propiedad intelectual e industrial respecto a la presente *Declaración de Prácticas de Certificación* y la información de la actividad de prestación de los servicios de certificación, respecto de los cuales se concede únicamente a los *Suscriptores* un derecho de uso.

Los *OID* propiedad de ANCERT 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 ANCERT salvo para los usos previstos en los *Certificados* o en el *Directorio 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 ANCERT pone a disposición de los *Suscriptores de Certificados*.

10 Ley aplicable, interpretación y jurisdicción competente

La presente *Declaración de Prácticas de Certificación* se rige por la Ley española en cuanto a su cumplimiento, interpretación, integración y validez, con independencia de su lugar de residencia o de donde sea utilizado el *Certificado* por los *Solicitantes y/o Suscriptores.*