POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS NOTARIALES DE SERVIDOR SEGURO

Versión 1.0
Fecha: 22/04/2004

Índice

1 INTRODUCCION 4

1.1. PRESENTACIÓN 4

1.2. IDENTIFICACIÓN 4

1.3. DIRECTORIO DE *CERTIFICADOS* 4

1.4. PUBLICACIÓN 5

1.5. FRECUENCIA DE ACTUALIZACIONES 5

1.6. CONTROL DE ACCESO AL DIRECTORIO DE *CERTIFICADOS* 5

2 DESCRIPCION DEL CERTIFICADO 5

2.1. ÁMBITO DE APLICACIÓN 5

2.2. TIPO DE CERTIFICADO 6

2.3. USOS DEL *CERTIFICADO* 6

2.4. LIMITACIONES DE USO 6

2.4.1 Usos prohibidos 6

3 IDENTIFICACION Y AUTENTICACION 7

3.1. NOMBRE DEL CERTIFICADO NOTARIAL DE SERVIDOR SEGURO 7

3.1.1 Nombre distintivo en el campo *Subject* del Certificado 7

3.1.2 Significado de los nombres del *Subject* 7

3.1.3 Interpretación del formato de nombres 7

3.1.4 Uso de nombres comerciales o marcas 7

3.1.5 Modificación de la denominación social de personas jurídicas 7

3.2. COMPROBACIÓN DE LA IDENTIDAD DE LOS SOLICITANTES 8

4 CICLO DE VIDA DEL CERTIFICADO 8

4.1. PRESOLICITUD 8

4.1.1 Presolicitud vía Web 9

4.1.2 Presolicitud ante Notario 9

4.2. SOLICITUD 9

4.2.1 Solicitante Persona Física 9

4.2.2 Solicitante Persona Jurídica 10

4.3. EMISIÓN 10

4.4. PUBLICACIÓN DEL CERTIFICADO 11

4.5. FORMALIZACIÓN DEL CONTRATO 11

4.6. COMPOSICIÓN DEL CERTIFICADO 11

4.6.1 Composición del nombre distintivo del *Subject* de Certificados Notariales de Servidor Seguro 11

4.6.2 Perfil del Certificado Notarial de Servidor Seguro 12

4.7. CADUCIDAD 13

4.8. EXTINCIÓN Y SUSPENSIÓN 13

4.8.1 Revocación 13

4.8.2 Suspensión 14
4.8.3 Levantamiento de la suspensión del *Certificado* 15
4.8.4 Procedimiento de Extinción 15
4.8.5 Efectos comunes de la extinción y suspensión 15
5 OBLIGACIONES Y RESPONSABILIDADES 16

1 INTRODUCCION

1.1. Presentación

El presente documento recoge la *Política de Certificación* de la Autoridad de Certificación **ANCERT Certificados Notariales de Sistemas** para los **Certificados Notariales de Servidor Seguro**. Esta Política de Certificación detalla y completa lo definido en la *Declaración de Prácticas de Certificación* de ANCERT, recogiendo su ámbito de aplicación, las características técnicas de este tipo de *Certificado*, el conjunto de reglas que indican los procedimientos seguidos en la prestación de servicios de certificación, tales como el ciclo de vida de los *Certificados*, así como sus condiciones de uso.

Esta Política de Certificación, junto con la *Declaración de Prácticas de Certificación* de ANCERT, está especialmente dirigida a cualquiera que confíe de buena fe en este tipo de *Certificados*.

Los conceptos y terminología de la presente *Política de Certificación* deberán interpretarse de acuerdo con el punto "1.8 Definiciones y Acrónimos" de la *Declaración de Prácticas de Certificación*.

ANCERT Certificados Notariales de Sistemas es la Autoridad de Certificación Subordinada para quien la Autoridad de Certificación raíz **ANCERT Certificados Notariales de Sistemas** ha expedido un certificado raíz para, a su vez, poder emitir los *Certificados* electrónicos **Certificados Notariales de Servidor Seguro**, previa identificación notarial, a personas físicas o jurídicas en calidad de titulares del nombre de dominio de servidores SSL.

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

1.2. Identificación

Política de Certificación de ANCERT de los **Certificados Notariales de Servidor Seguro**:

- *OID: 1.3.6.1.4.1.18920.1.2.1.1*

1.3. Directorio de *Certificados*

ANCERT Certificados Notariales de Sistemas dispone de un servicio de Directorio de *Certificado*s 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 dicha Autoridad de Certificación, el servicio se restablecerá en el estrictamente menor tiempo posible.

1.4. Publicación

ANCERT Certificados Notariales de Sistemas mantendrá el *Directorio de Certificados* que podrá ser consultado libremente vía Web las 24 horas de los 7 días de la semana en la dirección http://www.ancert.com. En el *Directorio de Certificados* de **ANCERT Certificados Notariales de Sistemas** se podrá consultar el estado de los *Certificado*s.

Así mismo podrán consultarse las Listas de Revocación de *Certificado*s (CRL), la presente Política de Certificación, la Declaración de Prácticas de Certificación y el *Certificado* Raíz de **ANCERT Certificados Notariales de Sistemas**.

1.5. Frecuencia de actualizaciones

Cuando **ANCERT Certificados Notariales de Sistemas,** en virtud de su actividad como *Prestador de Servicios de Certificación,* disponga de información actualizada la publicará oportunamente.

1.6. Control de Acceso al Directorio de *Certificados*

ANCERT Certificados Notariales de Sistemas no limita el acceso de lectura a las informaciones establecidas en los puntos 1.3 y 1.4 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 Certificados Notariales de Sistemas** utiliza sistemas fiables para el registro de *Certificado*s, pudiendo únicamente personas autorizadas hacer modificaciones.

2 DESCRIPCION DEL CERTIFICADO

2.1. Ámbito de aplicación

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.

2.2. Tipo de Certificado

Los **Certificados Notariales de Servidor Seguro** son *Certificados reconocidos,* en los términos del artículo 11 de la Ley 59/2003, de Firma Electrónica, es decir, son *Certificados* electrónicos expedidos por un Prestador de Servicios de Certificación cumpliendo los requisitos establecidos en dicha Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que prestan.

La *Firma Electrónica Reconocida* es la *Firma Electrónica Avanzada* basada en un certificado reconocido y que se genera mediante un *Dispositivo seguro de Creación de Firma*, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel. Los **Certificados Notariales de Servidor Seguro** incluyen los datos que exige el artículo 11 de la Ley 59.

2.3. Usos del *Certificado*

Los ***Certificados Notariales de Servidor Seguro*** se utilizan exclusivamente para realizar comunicaciones seguras y autenticadas entre servidor y cliente SSL, garantizando la autenticidad del servidor y la confidencialidad de los datos que se transmiten a través del canal de comunicaciones, entendiendo por ello lo siguiente:

Autenticidad de servidor

Asegura que la comunicación electrónica proviene del dispositivo de creación de firma del servidor del que dice provenir. El cliente de un servidor seguro puede verificarlo a través del **Certificados Notariales de Servidor Seguro** del *Suscriptor*.

Confidencialidad

Asegura que los datos que se transmiten no pueden ser leídos por terceras personas sin autorización, ya que los datos que se envían están cifrados.

2.4. Limitaciones de uso

2.4.1 Usos prohibidos

No se permite usar los ***Certificados Notariales de Servidor Seguro*** para usos diferentes a los previstos en los puntos 2.3. A titulo enunciativo, se prohíbe el uso de los **Certificados Notariales de Servidor Seguro** para:

1) fines contrarios al propio del mismo, a sus propósitos y funcionalidades, y a su correcta utilización.
2) firmar otro certificado o aplicaciones informáticas.
3) generar sellos de tiempo.
4) prestar servicios a título gratuito u oneroso, tales como servicios de OCSP, de facturación electrónica, de generación de *Listas de Revocación o de s*ervicios de notificación.

5) fines contrarios a la legislación vigente en España sobre prestación de servicios de certificación o firma electrónica en el momento de utilizar el Certificado.
6) fines contrarios a lo establecido en la Declaración de Prácticas de Certificación, en esta Política de Certificación y en el contrato de emisión de *Certificado Notarial Corporativo* firmado entre **ANCERT Certificados Notariales de Sistemas** y el Subscriptor del Certificado.

3 IDENTIFICACION Y AUTENTICACION

3.1. Nombre del Certificado Notarial de Servidor Seguro

En esta sección se establecen los requisitos relativos a los procedimientos de identificación y autenticación que han de utilizarse durante el registro de los Solicitantes de **Certificados Notariales de Servidor Seguro**, los cuales deben realizarse con anterioridad a la expedición de *Certificados*.

3.1.1 Nombre distintivo en el campo *Subject* del Certificado

Todos los **Certificados Notariales de Servidor Seguro** contienen un nombre distintivo X.500 en el campo Suscriptor - *Subject*, que incluye los campos que se desarrollan en el punto 4.6.1 de esta *Política de Certificación*.

3.1.2 Significado de los nombres del *Subject*

En los **Certificados Notariales de Servidor Seguro** el nombre del *Suscriptor* está compuesto por el nombre completo del dominio (FQDN) del servidor.

3.1.3 Interpretación del formato de nombres

Todos los nombres del *Suscriptor* están escritos utilizando lenguaje natural, prescindiendo de acentos. En ningún caso se pueden modificar, excepto para adaptarlos al formato y longitud del componente *CommonName* en el que se insertan.

3.1.4 Uso de nombres comerciales o marcas

No pueden utilizarse nombres comerciales o marcas para identificar a una persona jurídica.

3.1.5 Modificación de la denominación social de personas jurídicas

En caso de modificación de la denominación social de una persona jurídica, se deberá revocar el certificado electrónico existente a instancias del suscriptor y emitir un nuevo certificado electrónico que contenga la nueva denominación social.

3.2. Comprobación de la identidad de los Solicitantes

El proceso de identificación y autenticación se realizará exclusivamente mediante la personación del *Solicitante* ante un Notario español, que actuará como Autoridad de Registro, con la que **ANCERT Certificados Notariales de Sistemas** ha suscrito el Convenio correspondiente. El Notario documentará la solicitud del Certificado mediante la autorización de una Póliza que incluirá lo establecido en este documento.

Los tipos de documentos que son necesarios para acreditar la identidad del *Solicitante* pueden ser exclusivamente el Documento Nacional de Identidad, pasaporte, o cualquier otro medio admitido en derecho, siempre que contenga al menos la siguiente información:

a) Nombre y apellidos
b) Fecha de nacimiento
c) Numero de Identidad reconocido legalmente
d) Otros atributos del Solicitante

El documento necesario para acreditar al Notario la identidad de la persona jurídica es la escritura de constitución de la persona jurídica y el documento para acreditar la condición de representante de la persona jurídica es la escritura o documento público de donde derive la representación.

La acreditación necesaria para demostrar al notario la posesión del dominio público del servidor será la conexión on-line a cualquier registrador de dominios en Internet.

4 CICLO DE VIDA DEL CERTIFICADO

4.1. Presolicitud

Los *Certificado*s que incorporen firma electrónica reconocida se regirán en cuanto a los requisitos para su generación, entrega, conservación y revocación por lo que contractualmente se acuerde entre **ANCERT Certificados Notariales de Sistemas** y el *Suscriptor* del *Certificado*, con las especialidades que se contienen en la presente Política de Certificación.

La presolicitud de los *Certificado*s podrá realizarse a través de cualquier de los siguientes medios:

- Mediante acceso vía Web utilizando el aplicativo instalado en la página Web www.ancert.com, en cuyo caso el Solicitante deberá realizar una presolicitud del *Certificado*.

- Directamente mediante la presencia física ante un Notario que ha suscrito el correspondiente *Convenio* con **ANCERT Certificados Notariales de Sistemas** declarándole como Autoridad de Registro.

4.1.1 Presolicitud vía Web

El trámite de Presolicitud del *Certificado* se realizará mediante conexión a la Web http://.www.ancert.com y consistirá en las siguientes fases:

1. Siguiendo en cada caso las instrucciones indicadas en la Web, el *Solicitante* seleccionará el Notario que desea acudir para la emisión del *Certificado* comunicando los siguientes datos personales en un formulario: nombre, apellidos y dirección de correo electrónico.

2. El *Solicitante* recibirá de **ANCERT Certificados Notariales de Sistemas** una comunicación por correo electrónico donde se le solicitará que confirme la presolicitud, mediante un link a la Web de **ANCERT Certificados Notariales de Sistemas**.

3. El Solicitante debe clickear en el link proporcionado, donde aparecerán los requisitos de información y documentación que le serán solicitados en presencia notarial, junto con la tarifa del *Certificado*. A su vez, el Solicitante deberá seleccionar el medio de comunicación por el cual el Notario se pondrá en contacto con él para completar la presolicitud.

4. El Notario se pondrá en contacto con el *Solicitante* convocarlo a la notaría para continuar con el proceso de contratación, según el punto 4.1.1

4.1.2 Presolicitud ante Notario

El trámite de Presolicitud del Certificado podrá realizarse mediante personación directa ante un Notario que ha suscrito el correspondiente Convenio con **ANCERT Certificados Notariales de Sistemas** declarándole como Autoridad de Registro, el cual le informará de los requisitos de información y documentación para la solicitud del *Certificado*.

4.2. Solicitud

4.2.1 Solicitante Persona Física

En el supuesto de que el titular del nombre de dominio del servidor SSL sea una persona física, ésta deberá personarse ante Notario, el cual procederá a confirmar su identificación personal mediante Documento Nacional de Identidad (DNI) vigente, u otros medios admitidos en derecho a efectos de identificación descritos en el punto 3.2 de este documento.

La acreditación necesaria para demostrar al notario la posesión del dominio público del servidor será la conexión on-line a cualquier registrador de dominios en Internet.

De la intervención quedará constancia en la *Póliza* autorizada ante Notario.

En caso de que la documentación aportada por el compareciente sea insuficiente, el Notario no autorizará documento alguno ni solicitará la emisión del *Certificado*. Si el

Suscriptor quiere obtener el *Certificado* deberá comparecer de nuevo una vez subsanados los defectos y se seguirá lo establecido en el punto siguiente.

4.2.2 Solicitante Persona Jurídica

En el supuesto de que el titular del nombre de dominio del servidor SSL sea una persona jurídica el *Solicitante* deberá aportar los datos que acrediten su identidad personal, mediante los documentos señalados en el punto 3.2, así como documentar los datos relativos a la constitución y personalidad jurídica de la sociedad, y la extensión y vigencia de sus facultades de representación sobre la entidad representada, documento que tendrá una duración indefinida o temporal. En este último caso, el periodo no será nunca inferior a dos años.

El Notario calificará la suficiencia de las facultades comprobando los datos aportados por el *Solicitante*. El Notario comprobará dichos datos, bien mediante consulta en el Registro en el que estén inscritos los documentos de constitución y apoderamiento, bien mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, cuando aquellos no sean de inscripción obligatoria.

En el caso de realizar la consulta en el Registro Mercantil, aún en el supuesto de no constar debidamente inscritas las facultades, el Notario podrá autorizar el proceso de solicitud aplicando la legislación Mercantil para los representantes legales de sociedades (se incluye el caso que la acreditación de las facultades se documente en una Escritura autorizada por el Notario que actúe como Autoridad de Registro).

La consulta registral se efectuará comunicándose con el Registro Mercantil Central para que le trasmita la información mercantil suministrada por los Registros Mercantiles Provinciales de las sociedades mercantiles inscritas.

La acreditación necesaria para demostrar al notario la posesión del dominio público del servidor será la conexión on-line a cualquier registrador de dominios en Internet.

4.3. Emisión

Los trámites a seguir para la emisión de las claves y el *Certificado* del *Solicitante* son los siguientes:

- El *Solicitante* deberá presentar al Notario el archivo en formato *PKCS10* que contiene la petición de *Certificado*.
- El Notario procederá a introducir en el *Lector de Tarjetas* su *Tarjeta Criptográfica* con el *Certificado* que le autentica como Notario autorizado a emitir **Certificados Notariales de Servidor Seguro** y accederá a la aplicación de registro.
- El Notario comprobará, mediante las herramientas que le proporciona **ANCERT Certificados Notariales de Sistemas,** que el archivo facilitado por el *Solicitante* corresponde con la información aportada y con los campos solicitados en el punto 4.6.1 y 4.6.2.
- Si los datos son correctos completará el formulario de petición de *Certificado* y enviará la petición a **ANCERT Certificados Notariales de Sistemas.**

- En el plazo de 48 horas, el *Solicitante* podrá obtener su **Certificado Notarial de Servidor Persona Jurídica** descargándolo de la dirección www.ancert.com.
- El sistema generará automáticamente una factura, por el importe que consta en la Web de **ANCERT Certificados Notariales de Sistemas** www.ancert.com, según lo previsto en el punto 4.5,

Los *Datos de creación de Firma* permanecerán siempre bajo el exclusivo control del *Suscriptor* de los mismos, no guardándose copia de ellos ni **ANCERT Certificados Notariales de Sistemas** ni la Autoridad de Registro.

4.4. Publicación del *Certificado*

Un vez emitido el *Certificado* **ANCERT Certificados Notariales de Sistemas** publicará automáticamente una copia del mismo en el *Directorio de Certificados* de **ANCERT Certificados Notariales de Sistemas**.

4.5. Formalización del Contrato

Simultáneamente a la emisión del *Certificado*, el *Solicitante* en presencia del Notario, suscribirá una *Póliza* en la que el Notario, además de hacer constar los datos de identificación de la persona física anteriormente referidos, pondrá de manifiesto las facultades de la persona jurídica a la que se le va a conceder el *Certificado*, el ámbito de representación del *Solicitante*, así como los datos de inscripción en los registros públicos cuando estos fueren obligatorios y el Notario, por no ser el autorizante del documento de donde derive la representación, estuviere obligado a consignarlos.

Asimismo el clausulado contendrá en una remisión a la presente Política de Certificación y a la CPS, entregándosele por el Notario una copia de la *Póliza*.

4.6. Composición del *Certificado*

4.6.1 Composición del nombre distintivo del *Subject* de Certificados Notariales de Servidor Seguro

Los datos personales del Solicitante acreditados durante el proceso de solicitud del Certificado componen el nombre distintivo (DN) del Solicitante conforme al estándar X.500, la composición del cual es la siguiente:

Campo	***Descripción***	***Contenido***
EA	e-mail del *Suscriptor*	
CN	FQDN del Servidor propiedad del *Suscriptor*	Nombre del servidor y dominio

OU	Razón Social o Nombre y Apellidos del *Suscriptor* – CIF o NIF	
O	Tipo de Certificado	Certificado Notarial de Servidor Seguro
C	País	ES

Una vez compuesto el nombre distintivo que identificará al *Suscriptor*, se crea la correspondiente entrada en el directorio, asegurando que el nombre distintivo es único en toda la infraestructura del *Prestador de Servicios de Certificación*.

4.6.2 Perfil del Certificado Notarial de Servidor Seguro

Las extensiones utilizadas por los certificados emitidos bajo el amparo de la presente política son:

CAMPO	**VALOR**
Versión	V3
SerialNumber	2BFD 79E8 82A0 4B01 C818 5720 6614 6EFB
Issuer(Emisor)	
CommonName	ANCERT Certificados Notariales Sistemas
Organization	Agencia Notarial de Certificacion S.L. Unipersonal - CIF B83395988
Locality	Paseo del General Martinez Campos 46-6a planta
State	Madrid
Country	ES
Valido desde	La fecha de emisión
Valido hasta	Dos años después de la emisión
Clave Pública	Octet String Conteniendo la clave pública del suscriptor
Extended Key Usage	TLS web server authentication (OID 1.3.6.1.5.5.7.3.1)
CRL Distribution Points	Distribution Point Name (uRI) “http://www.ancert.com/crl/ANCERTCS.crl" “http://www2.ancert.com/crl/ ANCERTCS.crl" “http://www3.ancert.com/crl/ ANCERTCS.crl"
Certificate Policy Extensions	
PolicyIdentifier	1.3.6.1.4.1.18920.1.2.1.1
CPSuri	http://www.ancert.com/cps
Usernotice	Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. La declaración de políticas de certificación que rige el funcionamiento de este certificado se encuentra disponible en http://www.ancert.com/cps
Key Usage	digital signature key encipherment data encipherment
Netscape Certificate Type	SSL server

Basic Contraints	Ca False Path Lengh Constraint 0
Authority Key Identifier	84F7 FA72 5E88 6466 1D28 8CB0 77BD 0C6A 9F4C 4D62
Algoritmo de firma	sha1RSA
Authority Information Access	
AccessMethod	1.3.6.1.5.5.7.48.1
accessLocation	uRI = http://ocsp.ac.ancert.com/ocsp.xuda

4.7. Caducidad

Los *Certificados* emitidos por **ANCERT Certificados Notariales de Sistemas** tendrán un periodo de validez de dos (2) años contados a partir del momento de la emisión del *Certificado*, sin perjuicio de que durante su vigencia concurra cualquier causa de extinción de las establecidas en la *Declaración de Prácticas de Certificación*.

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 Certificados Notariales de Sistemas**. Ésta notificará al Suscriptor, mediante correo electrónico, la expiración de sus *Certificado*s con una antelación de un mes. Tal notificación se realiza exclusivamente para la conveniencia del notificado en el proceso de obtención de un nuevo *Certificado*. Transcurrido este período el *Certificado* caducará.

El *Certificado* tendrá efectos frente a terceros de buena fe desde el momento de su publicación en el *Directorio de Certificados* de **ANCERT Certificados Notariales de Sistemas**.

4.8. Extinción y suspensión

4.8.1 Revocación

Los ***Certificados Notariales de Servidor Seguro*** son revocables. En cuanto a los sujetos que pueden solicitar la revocación, las causas y los efectos de la misma y el momento de producción de tales efectos, se estará a lo dispuesto en la CPS de ANCERT.

El procedimiento de revocación de los ***Certificados Notariales de Servidor Seguro*** será diferente en función del origen de la solicitud de revocación:

- En el caso de que provenga de cualquier representante del *Suscriptor*, éste deberá personarse ante un Notario que ha suscrito el correspondiente *Convenio* con **ANCERT Certificados Notariales de Sistemas** declarándole como Autoridad de Registro, el representante del Suscriptor deberá identificarse de acuerdo al procedimiento definido en el punto 3.2 de este documento. El Notario autorizará una *Póliza* de Revocación del *Certificado*, de la cual deberá remitir una copia a **ANCERT Certificados Notariales de**

Sistemas. El notario solicitará la revocación accediendo a la aplicación telemática de revocación de **ANCERT Certificados Notariales de Sistemas**.

En este supuesto el Notario deberá comprobar que el representante del suscriptor ostenta facultades suficientes para revocar aquellas que fueron alegadas por el *Solicitante* en el momento de la obtención del *Certificado.*

- En el caso de que provenga a iniciativa de **ANCERT Certificados Notariales de Sistemas,** éste únicamente podrá proceder a la revocación del *Certificado* cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en la CPS de ANCERT.

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

En ningún caso cabe la solicitud de revocación de un *Certificado* mediante envío de correo electrónico, ni por ningún otro medio excepto los anteriormente descritos.

4.8.2 Suspensión

Los ***Certificados Notariales de Servidor Seguro*** pueden ser suspendidos. En cuanto a los sujetos que pueden solicitar la suspensión, las causas y los efectos de la misma y el momento de producción de tales efectos, se estará a lo dispuesto en la CPS de ANCERT.

El procedimiento de suspensión de los ***Certificados Notariales de Servidor Seguro*** será diferente en función del origen de la solicitud de revocación:

- A solicitud del Suscriptor. El legítimo solicitante deberá telefonear al número 902 348 347 de Centro de Atención a Usuarios de **ANCERT Certificados Notariales de Sistemas**. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante de la suspensión será sometida a grabación. El solicitante de la suspensión deberá responder con la contraseña que hubiera hecho constar a estos efectos en el proceso de Solicitud del *Certificado*. En caso de que la respuesta coincida con dicha contraseña el operador procederá a suspender el *Certificado*.

  Transcurrido un tiempo superior a 60 días, desde que se incluya la suspensión en la Lista de Revocación, sin que el Suscriptor haya solicitado su levantamiento, **ANCERT Certificados Notariales de Sistemas** podrá revocar el *Certificado*.

- En el caso de que provenga a instancia de **ANCERT Certificados Notariales de Sistemas,** éste únicamente podrá proceder a la suspensión del *Certificado* cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en la CPS de ANCERT.

Transcurrido un tiempo superior a 60 días, desde que se incluya la suspensión en la Lista de Revocación, sin que el Suscriptor haya solicitado su levantamiento, **ANCERT Certificados Notariales de Sistemas** podrá revocar el *Certificado*.

En todos los casos, una vez suspendido el *Certificado*, la suspensión será publicada en el *Directorio de Certificados* de ANCERT, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la *Lista de Certificados Revocados* (CRL) en el plazo máximo previsto de veinticuatro (24) horas.

En ningún caso cabe solicitar la suspensión de un *Certificado* mediante envío de correo electrónico, ni por ningún otro medio excepto los anteriormente descritos.

4.8.3 Levantamiento de la suspensión del *Certificado*

Los *Suscriptores* podrán solicitar el levantamiento de la suspensión durante los sesenta (60) días siguientes a su suspensión debiendo telefonear al teléfono 902 348 347 del Centro de Atención a Usuarios de **ANCERT Certificados Notariales de Sistemas**. A los efectos probatorios oportunos, la conversación entre el operador y el solicitante será sometida a grabación. El solicitante del levantamiento de la suspensión deberá responder con la contraseña que hubiera hecho constar a estos efectos en el proceso de Solicitud del *Certificado*. En caso de que la respuesta coincida con dicha contraseña el operador procederá a levantar la suspensión del *Certificado*.

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

En el caso de que la suspensión haya provenido de **ANCERT Certificados Notariales de Sistemas,** éste únicamente podrá proceder a levantar la suspensión del *Certificado* cuando por medio fehaciente halla tenido conocimiento cierto de la desaparición de la causa que motivó la suspensión. En este caso, inmediatamente después procederá a eliminar el *Certificado* de la *Lista de Revocación.*

4.8.4 Procedimiento de Extinción

ANCERT Certificados Notariales de Sistemas extinguirá el *Certificado,* además de los casos de revocación descritos, cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las restantes causas de extinción enumeradas en la CPS de ANCERT.

4.8.5 Efectos comunes de la extinción y suspensión

En los casos de extinción de *Certificados,* por causa de revocación o cualquier otra de las previstas en la CPS de ANCERT o en la Ley, o en los casos de suspensión, **ANCERT Certificados Notariales de Sistemas** hará constar inmediatamente en el *Directorio de Certificados y* cada veinticuatro (24) horas en la *Lista de Revocación de*

Certificado, exceptuando en este caso la caducidad del *Certificado*, la extinción o suspensión de la vigencia de los *Certificado*s electrónicos en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

La extinción o suspensión de la vigencia de un *Certificado* electrónico no tendrá efectos retroactivos.

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

5 Obligaciones y responsabilidades

Sin perjuicio de las obligaciones y responsabilidades particulares establecidas en la presente *Política de Certificación*, las partes participantes en la actividad de certificación de **ANCERT Certificados Notariales de Sistemas** deberán cumplir lo previsto en los puntos “6 OBLIGACIONES” y “7 RESPONSABILIDADES” de la *Declaración de Prácticas de Certificación*.