



POLÍTICA DE CERTIFICACIÓN DE CERTIFICADOS PARA EMPLEADOS

Versión 1.0
Fecha: 25/10/2004

Índice

1	INTRODUCCION	4
1.1.	PRESENTACIÓN	4
1.2.	IDENTIFICACIÓN	4
1.3.	DIRECTORIO DE <i>CERTIFICADOS</i>	5
1.4.	PUBLICACIÓN	5
1.5.	FRECUENCIA DE ACTUALIZACIONES	5
1.6.	CONTROL DE ACCESO AL <i>DIRECTORIO DE CERTIFICADOS</i>	5
2	DESCRIPCIÓN DEL <i>CERTIFICADO</i>	6
2.1.	ÁMBITO DE APLICACIÓN	6
2.2.	TIPO DE <i>CERTIFICADO</i>	6
2.3.	USOS DEL <i>CERTIFICADO</i>	6
2.3.1	Uso permitido del Certificado	7
2.4.	LIMITACIONES DE USO	7
2.4.1	Usos prohibidos	7
2.4.2	Limitación de cuantías	7
3	IDENTIFICACION Y AUTENTICACION	8
3.1.	NOMBRE DEL CERTIFICADO PARA EMPLEADOS	8
3.1.1	Nombre distintivo en el campo <i>Subject</i> del <i>Certificado</i>	8
3.1.2	Identidad alternativa en el campo <i>Subject</i> del <i>Certificado</i>	8
3.1.3	Nombre del <i>Suscriptor</i> persona física	8
3.1.4	Uso de pseudónimos	8
3.1.5	Interpretación del formato de nombres	8
3.2.	COMPROBACIÓN DE LA IDENTIDAD DE LOS <i>SUSCRIPTORES</i>	8
4	CICLO DE VIDA DEL <i>CERTIFICADO</i>	9
4.1.	SOLICITUD	9
4.2.	EMISIÓN	9
4.3.	PUBLICACIÓN DEL <i>CERTIFICADO</i>	10
4.4.	ENTREGA DEL CERTIFICADO	11
4.5.	COMPOSICIÓN DEL <i>CERTIFICADO</i>	11
4.5.1	Composición del nombre distintivo del Subject de Certificados para Empleados	11
4.5.2	Composición de la identidad alternativa del <i>Subject</i> de <i>Certificados para Empleados</i>	11
4.5.3	Perfil del Certificado para empleados	12
4.6.	CADUCIDAD	13
4.7.	EXTINCIÓN Y SUSPENSIÓN	13
4.7.1	Revocación	13
4.7.2	Suspensión	14

4.7.3	Levantamiento de la suspensión del <i>Certificado</i>	14
4.7.4	Procedimiento de Extinción	14
4.7.5	Efectos comunes de la extinción y suspensión.....	15
5	OBLIGACIONES Y RESPONSABILIDADES	15

1 INTRODUCCION

1.1. Presentación

El presente documento recoge la *Política de Certificación* de la Autoridad de Certificación **ANCERT Certificados para Empleados** para los **Certificados para Empleados**. 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 para empleados es la Autoridad de Certificación subordinada para quien la Autoridad de Certificación raíz **ANCERT Certificados CGN** ha expedido un *Certificado* raíz para, a su vez, poder emitir los *Certificados* electrónicos **Certificados para Empleados**.

ANCERT Certificados para empleados emite los **Certificados para Empleados** para todos los empleados de Notarías y Colegios Notariales del territorio español. El Notario para los empleados de notaría y los Colegios Notariales para los empleados de los mismos, (en adelante la *Autoridad de Registro*) son responsables de la identificación de su identidad.

Se utilizan Tarjetas *Criptográficas* como único soporte de los *Certificados*.

Los **Certificados para Empleados** 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 59/2003 de Firma Electrónica.

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

1.2. Identificación

Política de Certificación de **ANCERT Certificados CGN** de los **Certificados para Empleados**:

- *OID: 1.3.6.1.4.1.18920.4.2.1.1*

1.3. Directorio de *Certificados*

ANCERT Certificados para empleados dispone de un servicio de 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 dicha Autoridad de Certificación, el servicio se restablecerá en el estrictamente menor tiempo posible.

1.4. Publicación

ANCERT Certificados para empleados 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 para empleados** se podrá consultar el estado de los *Certificados*.

Así mismo podrán consultarse las *Listas Certificados Revocados*, la presente *Política de Certificación*, la *Declaración de Prácticas de Certificación* y el *Certificado* raíz de **ANCERT Certificados para empleados**.

1.5. Frecuencia de actualizaciones

Cuando **ANCERT Certificados para empleados**, 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 para empleados 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 para empleados** utiliza sistemas fiables para el registro de *Certificados*, pudiendo únicamente personas autorizadas hacer modificaciones.

2 DESCRIPCIÓN DEL *CERTIFICADO*

2.1. *Ámbito de aplicación*

ANCERT Certificados para empleados expide los **Certificados para Empleados** a personas físicas, en su nombre propio. Podrán contener o no atributos cumpliendo los requisitos señalados en esta *Política Certificación*.

2.2. *Tipo de Certificado*

Los **Certificados para Empleados** 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 Ley sólo considera Firma Electrónica reconocida la firma electrónica avanzada basada en un *Certificado reconocido* y generada mediante un *Dispositivo seguro de creación de Firma*. Por ello, la firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

2.3. *Usos del Certificado*

Los **Certificados para Empleados** se utilizan para la Firma electrónica reconocida de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor, el no repudio de origen y la integridad del contenido, entendiendo por ello lo siguiente:

Autenticidad de origen

Asegura que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona o entidad de quien dice provenir. Esta característica se obtiene mediante la firma electrónica reconocida. El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del **Certificado para Empleados** del *Suscriptor*.

No repudio de origen

Evita que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo. Para ello se utiliza la firma electrónica reconocida. El receptor de un mensaje firmado digitalmente puede verificar esa firma a través del **Certificado para Empleados** del *Suscriptor*. De esta forma puede demostrar la identidad del emisor del mensaje sin que éste pueda repudiarlo.

Integridad

Permite comprobar que un documento electrónico firmado con *Firma electrónica reconocida* no ha sido modificado por ningún agente externo. Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (funciones de *hash*), utilizadas en combinación con la firma electrónica. El procedimiento se centra en firmar electrónicamente un resumen único del documento electrónico con la clave privada del suscriptor de forma que cualquier alteración del documento revierte en una alteración de su resumen.

2.3.1 Uso permitido del Certificado

Podrá utilizarse el **Certificado para Empleados** para cifrar o descifrar documentos electrónicos bajo su exclusiva responsabilidad. Todas las responsabilidades legales, contractuales o extra contractuales, daños directos o indirectos que puedan derivarse de tales usos quedan a cargo del *Suscriptor*. En ningún caso podrán *las Autoridades de Registro* ni el *Suscriptor* ni los terceros perjudicados reclamar a **ANCERT Certificados para empleados** compensación o indemnización alguna por daños o responsabilidades provenientes del uso de las claves o los *Certificados* para fines de cifrado de confidencialidad.

2.4. Limitaciones de uso

2.4.1 Usos prohibidos

No se permite usar los **Certificados para Empleados** para usos diferentes a los previstos en los puntos 2.3 y 2.3.1. A título enunciativo, se prohíbe el uso de los **Certificados para Empleados** 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 servicios 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*.

2.4.2 Limitación de cuantías

Los **Certificados para Empleados** emitidos por **ANCERT Certificados para empleados** se conceden sin limitación de uso por razón de la cuantía.

3 IDENTIFICACION Y AUTENTICACION

3.1. Nombre del Certificado para Empleados

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

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

Todos los **Certificados para Empleados** contienen un nombre distintivo X.500 en el campo *Subject*, que incluye los campos que se desarrollan en el punto 4.5.1 de esta *Política de Certificación*.

3.1.2 Identidad alternativa en el campo *Subject* del *Certificado*

Todos los **Certificados para Empleados** contienen una identidad alternativa X.500 en el campo *Subject*, que incluye los campos que se desarrollan en el punto 4.5.2 de esta *Política de Certificación*.

3.1.3 Nombre del *Suscriptor* persona física

En los **Certificados para Empleados** el nombre del *Suscriptor* está compuesto únicamente por su nombre y apellidos.

3.1.4 Uso de pseudónimos

No pueden utilizarse pseudónimos para identificar a una persona física.

3.1.5 Interpretación del formato de nombres

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

3.2. Comprobación de la identidad de los *Suscriptores*

El proceso de identificación y autenticación lo realizarán, como *Autoridad de Registro*, exclusivamente los Notarios o el Colegio Notarial, según corresponda.

Los tipos de documentos que son necesarios para acreditar la identidad del *Suscriptor* 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) Lugar y fecha de nacimiento
- c) Numero de Identidad reconocido legalmente
- d) Otros atributos del Solicitante

El documento necesario para acreditar la relación laboral con la Notaría o con el Colegio Notarial es el contrato laboral en vigor.

4 CICLO DE VIDA DEL *CERTIFICADO*

4.1. Solicitud

Los *Certificados* que incorporen firma electrónica reconocida se registrarán en cuanto a los requisitos para su solicitud, generación, entrega, conservación y revocación por lo que contractualmente se acuerde entre **ANCERT Certificados para empleados** y la *Autoridad de Registro*, con las especialidades que se contienen en la presente *Política de Certificación*.

En todo caso, previamente a efectuar la solicitud del *Certificado*, la *Autoridad de Registro* identificará a los *Suscriptores* mediante el Documento Nacional de Identidad vigente, u otros medios admitidos en derecho a efectos de identificación descritos en el punto 3.2 de este documento.

4.2. Emisión

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

Certificados para empleados de Notaría:

1. El Notario actuará como *Autoridad de Registro* identificando a sus empleados y solicitando la emisión del *Certificado* al Colegio Notarial correspondiente.
2. Los Colegios Notariales accederán a la aplicación de emisión de certificados de **ANCERT Certificados para empleados** utilizando un *Certificado* que los autentique.
3. Una vez autenticado, el Oficial encargado introducirá en el Lector de Tarjetas la *Tarjeta Criptográfica* del empleado, que previamente le ha sido entregada junto a los códigos PIN y PUK correspondientes en sobre cerrado.
4. El Oficial encargado completará el formulario de registro con los datos del empleado y solicitarán la emisión del *Certificado*.
5. En este momento, la aplicación de registro solicitará el PIN correspondiente a la *Tarjeta Criptográfica* del empleado, para activar el procedimiento de generación de claves.
6. En ese momento se generará el par de claves en la *Tarjeta Criptográfica* del empleado, enviando la petición a **ANCERT Certificados para empleados**, la cual generará el *Certificado* y lo remitirá vía SSL al ordenador del Oficial

encargado, quedando almacenado automáticamente en la *Tarjeta Criptográfica* del empleado.

Certificados para empleados de Colegio Notarial:

1. El Colegio Notarial actuará como *Autoridad de Registro* identificando a sus empleados.
2. El Oficial encargado accederá a la aplicación de emisión de certificados de **ANCERT Certificados para empleados** utilizando un *Certificado* que le autentique.
3. Una vez autenticado, introducirá en el Lector de Tarjetas la *Tarjeta Criptográfica* del empleado de Colegio Notarial, que previamente le ha sido entregada junto a los códigos PIN y PUK correspondientes en sobre cerrado.
4. El Oficial encargado completará el formulario de registro con los datos del empleado y solicitarán la emisión del *Certificado*.
5. En este momento, la aplicación de registro solicitará el PIN correspondiente a la *Tarjeta Criptográfica* del empleado, para activar el procedimiento de generación de claves.
6. En ese momento se generará el par de claves en la *Tarjeta Criptográfica* del empleado, enviando la petición a **ANCERT Certificados para empleados**, la cual generará el *Certificado* y lo remitirá vía SSL al ordenador del Oficial encargado, quedando almacenado automáticamente en la *Tarjeta Criptográfica* del empleado.

El soporte para el almacenamiento de las claves y el *Certificado* será siempre una *Tarjeta Criptográfica*, considerada como un *Dispositivo seguro de creación de firma*, con capacidades criptográficas de generación de los *Datos de creación y de verificación de Firma* lo que permite garantizar que la clave privada no abandona nunca la Tarjeta Criptográfica y que por lo tanto la Tarjeta Criptográfica no puede ser duplicada. Para realizar una firma o activar la tarjeta es necesario introducir el Código Secreto de Activación (PIN) que solamente debe conocer el Suscriptor de la Tarjeta. Tres intentos consecutivos erróneos en la introducción del PIN provocan un bloqueo de la Tarjeta. Para desbloquear la Tarjeta, el *Suscriptor* deberá introducir el código PUK y del mismo modo tres intentos consecutivos erróneos en la introducción del PUK provocan el bloqueo irreversible de la Tarjeta.

La creación de las claves Pública y Privada (1024 bits RSA) la realiza la propia tarjeta internamente, de tal forma que se garantiza tanto la robustez de las claves como la imposibilidad de un compromiso de las mismas en el proceso de generación.

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

4.3. Publicación del *Certificado*

Una vez emitido el *Certificado* **ANCERT Certificados para empleados** publicará automáticamente una copia del mismo en el *Directorio de Certificados* de **ANCERT Certificados para empleados**.

4.4. Entrega del Certificado

Una vez emitido el certificado, el Notario por cuenta del empleado de notaría o bien el representante del Colegio Notarial, en el caso de empleado de Colegio Notarial, recibirán las *Tarjetas Criptográficas* firmando la correspondiente acta de entrega.

4.5. Composición del *Certificado*

4.5.1 Composición del nombre distintivo del Subject de Certificados para Empleados

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:

En el siguiente cuadro se distingue el perfil de empleado de notaría y el de empleado de Colegio Notarial:

Campo	Descripción (Empleado Notaría)	Descripción (Empleado Colegio Notarial)
SN	NIF del empleado	NIF del empleado
CN	Nombre Completo del empleado	Nombre Completo del empleado
GN	Nombre del empleado	Nombre del empleado
SU	Apellidos del empleado	Apellidos del empleado
EA	Correo electrónico empleado	Correo electrónico empleado
OU	Código de notaría	Código Colegio
OU	Colegio Notarial	Colegio Notarial
OU		Cargo
O	EMPLEADO DE NOTARIA	EMPLEADO DE COLEGIO NOTARIAL
L	Población	Población
ST	Provincia	Provincia
C	País	País

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*.

4.5.2 Composición de la identidad alternativa del Subject de Certificados para Empleados

Campo	Descripción (Empleado Notaría)	Descripción (Empleado Colegio)
-------	--------------------------------	--------------------------------

		Notarial)
eMail	eMail empleado	eMail empleado

4.5.3 Perfil del Certificado para empleados

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

CAMPO	VALOR
Versión	V3
SerialNumber	6AB6 A756 D48E 3FA6 8A41 CF09 E391 84A2
Issuer(Emisor)	
CommonName	ANCERT Certificados para empleados
Organization	Agencia Notarial de Certificación S.L. Unipersonal - CIF B83395988
Locality	Paseo del General Martínez Campos 46-6a planta
State	Madrid
Country	ES
Valido desde	La fecha de emisión
Valido hasta	Tres años después de la emisión
Clave Pública	Octet String Contienindeo la clave pública del suscriptor
Extended Key Usage	TLS web client authentication (OID 1.3.6.1.5.5.7.3.2)
CRL Distribution Points	Distribution Point Name (uRI) "http://www.ancert.com/crl/ANCERTCE.crl" "http://www2.ancert.com/crl/ ANCERTCE.crl" "http://www3.ancert.com/crl/ ANCERTCE.crl"
Certificate Policy Extensions	
PolicyIdentifier	1.3.6.1.4.1.18920.4.2.1.1
CPSuri	http://www.ancert.com/cps
Usernotice	'Este certificado se expide como Certificado Reconocido de acuerdo con la legislación vigente. La declaración de prácticas de certificación y la política de certificación que rigen el funcionamiento de este certificado se encuentran disponibles en http://www.ancert.com'
Key Usage	digital signature
Netscape Certificate Type	SSL client
Basic Constraints	Ca False Path Length Constraint 0
Authority Key Identifier	EC57 9FC8 7622 6FCC 3AAE 5BF0 2DA1 6258 D18D 02CC
Authority Information Access	

AccessMethod	1.3.6.1.5.5.7.48.1
accessLocation	uRI = http://ocsp.ac.ancert.com/ocsp.xuda
Algoritmo de firma	sha1RSA

4.6. Caducidad

Los *Certificados* emitidos por **ANCERT Certificados para empleados** tendrán un periodo de validez de tres (3) 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 *Certificados* 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 para empleados**. Ésta notificará al *Suscriptor*, mediante correo electrónico, la expiración de sus *Certificados* 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 para empleados**.

4.7. Extinción y suspensión

4.7.1 Revocación

Los **Certificados para Empleados** 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.

La solicitud de revocación de los **Certificados para Empleados** se realizará:

- A solicitud de *la Autoridad de Registro*. Ésta podrá solicitar la revocación de los certificados emitidos, o bien
- A instancia de **ANCERT Certificados para empleados** la cual podrá proceder a la revocación del *Certificado* cuando por medio fehaciente haya tenido conocimiento cierto de la concurrencia con respecto al mismo de alguna de las causas de revocación enumeradas en 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 para empleados**, produciendo desde ese mismo instante efectos respecto a terceros, e incluida en la *Lista de Certificados Revocados* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.2 Suspensión

Los **Certificados para Empleados** 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.

La solicitud de suspensión de los **Certificados para Empleados** se realizará:

- A solicitud de *la Autoridad de Registro*. Ésta podrá solicitar la suspensión los certificados emitidos, o bien
- **ANCERT Certificados para empleados** 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.

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* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.3 Levantamiento de la suspensión del *Certificado*

La *Autoridad de Registro* podrá proceder a la solicitud del levantamiento de la suspensión durante los sesenta (60) días siguientes a su suspensión en caso de que el *Certificado* haya sido suspendido por *la Autoridad de Registro*.

En el caso de que la suspensión haya provenido de **ANCERT Certificados para empleados**, ésta 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 Certificados Revocados*.

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* en el plazo máximo previsto de veinticuatro (24) horas.

4.7.4 Procedimiento de Extinción

ANCERT Certificados para empleados 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.

4.7.5 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 para empleados** hará constar inmediatamente en el *Directorio de Certificados* y cada veinticuatro (24) horas en la *Lista de Revocación de Certificados*, exceptuando en este caso la caducidad del Certificado, la extinción o suspensión de la vigencia de los *Certificados* electrónicos en cuanto tenga conocimiento fundado de cualquiera de los hechos determinantes de la extinción o suspensión de su vigencia.

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 electrónica 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.

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 Certificados Revocados* 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*, los *Suscriptores*, las *Autoridades de Registro*, **ANCERT Certificados para Empleados**, los *Terceros de confianza*, y en general todas las partes participantes en la actividad de certificación de los **Certificados para Empleados** deberán cumplir lo previsto en los puntos “6 OBLIGACIONES” y “7 RESPONSABILIDADES” de la *Declaración de Prácticas de Certificación*.