

## **CONDICIONES DE USO**

APLICABLES A

### **CERTIFICADOS PERSONALES DE CORPORACIONES DE DERECHO PÚBLICO DE FIRMA ELECTRÓNICA RECONOCIDA**

Antes de verificar el certificado electrónico, o de acceder o utilizar la información del estado de certificados y el resto de información contenida en el Depósito de ANCERT, Usted (en lo sucesivo, "el verificador") tiene que leer y aceptar estas condiciones de uso.

Si el verificador comprueba un certificado electrónico, accede o utiliza la información del estado de certificados y el resto de información contenida en el Depósito de ANCERT, se entenderá que acepta todas las cláusulas de estas condiciones de uso.

## **CLÁUSULAS**

### **PRIMERA.** - *Objeto*

1. Estas condiciones de uso regulan la prestación por ANCERT de los servicios de información sobre los certificados, el estado de los certificados y otras informaciones publicadas en el Depósito, en relación con los certificados descritos en la cláusula tercera de estas condiciones de uso.
2. Estas condiciones de uso proporcionan garantías limitadas al servicio ofrecido, excluye cualquier otra garantía, así como toda responsabilidad que no derive del servicio de certificación ofrecido al verificador.

### **SEGUNDA.** - *DPC y documentación de operaciones de ANCERT*

1. Los Servicios de Certificación de ANCERT objeto de las presentes condiciones de uso, se regulan técnicamente y operativamente por la Declaración de Prácticas de Certificación de la Entidad de Certificación ANCERT Certificados de Corporaciones de Derecho Público (en lo sucesivo, la DPC) y sus actualizaciones posteriores, así como por documentación complementaria, publicadas para dar cumplimiento al artículo 19 de la Ley 59/2003, sobre firma electrónica, en la siguiente dirección de Internet:  
[<https://www.ancert.com/condiciones/>]
2. La DPC y la documentación de operaciones de ANCERT, modificadas periódicamente, se incorporan a las presentes condiciones de uso por referencia. El verificador declara conocer la última versión de la DPC, cuyos aspectos jurídicos descritos en la misma se contienen en su totalidad en estas condiciones de uso.
3. El verificador se compromete a cumplir con los requisitos técnicos, operativos y de seguridad descritos en la DPC y en la documentación de operaciones de ANCERT.

4. En caso de discrepancia, el significado de los términos contenidos en las presentes condiciones de uso prevalecerá sobre aquello establecido en la DPC.

**TERCERA.** - *Descripción del certificado personal de Corporación de Derecho Público de firma.*

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

La clase “Certificados Personales de Corporaciones de Derecho Público” agrupa los certificados expedidos por la Agencia Notarial de Certificación a corporaciones de Derecho Público, actuando éstas como Entidades de Registro de sus usuarios.

Los Certificados Personales de Corporaciones de Derecho Público permiten tres funcionalidades, emitiéndose un Certificado para cada una de ellas:

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

Los Certificados Personales de Corporaciones de Derecho Público pueden contener, además de los datos de identidad del suscriptor, los datos del poseedor de claves a los que se refiere el artículo 11 de la Ley 59/2003 de Firma Electrónica según lo dispuesto en la DPC.

Se utiliza una tarjeta criptográfica con la garantía de dispositivo seguro de creación de firma, en los términos del artículo 24 de la Ley 59/2003, de Firma Electrónica.

La tarjeta suministrada contiene tres certificados, diferenciados por el uso a que pueden destinarse:

- Certificado Personal de Corporación de Derecho Público de firma electrónica reconocida.
- Certificado Personal de Corporación de Derecho Público de autenticación.
- Certificado Personal de Corporación de Derecho Público de cifrado.

El Certificado Personal de Corporación de Derecho Público de firma electrónica reconocida se utiliza para la firma electrónica reconocida de documentos electrónicos o mensajes electrónicos, garantizando la autenticidad del emisor entendiendo por ello el aseguramiento de que el documento o la comunicación electrónica provienen del dispositivo de creación de firma de la persona de quien dice provenir.

Los Certificados Personales de Corporación de Derecho Público de firma electrónica reconocida se utilizan también para garantizar la integridad del contenido, entendiendo por ello que permiten comprobar que un documento electrónico no ha sido modificado por ningún agente externo.

Para garantizar la integridad, la criptografía utiliza las capacidades matemáticas de las funciones de resumen (en inglés, unciones de *hash*), utilizadas en combinación con la firma digital. El procedimiento se centra en firmar digitalmente un resumen único del documento electrónico con la clave privada del poseedor de claves de forma que cualquier alteración del documento revierte en una alteración de su resumen.

Además de los anteriores aspectos, sólo los Certificados Personales de Corporación de Derecho Público de firma electrónica reconocida garantizan la irrefutabilidad de los mensajes, basada en el conocimiento de su contenido (función también denominada "no repudio de origen"), entendiendo por ello evitar que el emisor de un determinado mensaje pueda negar, si ello le conviene, la emisión del mismo o su contenido.

Esta característica se obtiene mediante la firma electrónica reconocida, que es la firma electrónica avanzada basada en un certificado reconocido y que se genera mediante un dispositivo seguro de creación de firma, teniendo respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

El receptor de un mensaje firmado electrónicamente puede verificar esa firma a través del Certificado Personal de Corporación de Derecho Público de firma electrónica reconocida del suscriptor.

Los Certificados Personales de Corporación de Derecho Público de firma electrónica reconocida se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.18920. 3.1.1.2.1

No se permite usar los Certificados Personales de Corporaciones de Derecho Público de firma electrónica reconocida, para usos diferentes a los previstos supra. A título enunciativo, se prohíbe el uso de los Certificados Personales de Corporaciones de Derecho Público firma electrónica reconocida 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 DPC y las presentes Condiciones Generales de Uso.

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

Los Certificados Personales de Corporaciones de Derecho Público de firma electrónica reconocida, emitidos por ANCERT Certificados para Corporaciones de Derecho Público se conceden sin limitación de uso por razón de la cuantía.

#### Propiedad Intelectual

El verificador reconoce que ANCERT es el dueño de todos los certificados emitidos, así como de las especificaciones, tarjetas y marcas, sin perjuicio de los derechos de terceros.

#### Duración del Certificado

Los Certificados Personales de Corporaciones de Derecho Público tendrán un periodo máximo de validez de tres (3) años a contar desde el día de su emisión, a partir del cual no podrán ser utilizados.

La fecha de expiración de los certificados figurará indicada en los propios certificados.

### **CUARTA. - Obligaciones del verificador**

#### 1. Decisión informada

ANCERT informa al verificador, que se da por notificado, que tiene acceso a información suficiente para tomar una decisión informada en el momento de verificar un certificado y confiar en la información contenida en el certificado.

Adicionalmente, el verificador reconoce que el uso del Depósito y de las Listas de Revocación de Certificados (en lo sucesivo, "las CRLs") de ANCERT, se rige por la DPC de la Entidad de Certificación ANCERT Certificados para Corporaciones de Derecho Público, y se compromete a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

#### 2. Requisitos de verificación de la firma electrónica

Para confiar en un mensaje o documento, el verificador tiene que validar dos firmas:

- En primer lugar, tiene que verificar la firma electrónica del mensaje o documento. Esta comprobación es imprescindible para determinar que fue generada por el suscriptor, utilizando la clave privada correspondiente a la clave pública contenida en el Certificado

Personal de Corporaciones de Derecho Público, y para garantizar que el mensaje o documento firmado no fue modificado desde la generación de la firma electrónica.

- En segundo lugar, tiene que verificar la firma electrónica del Certificado Personal de Corporaciones de Derecho Público del suscriptor. Esta comprobación es imprescindible para determinar que la clave pública contenida en el Certificado Personal de Corporaciones de Derecho Público corresponde al suscriptor.

Esta comprobación será ejecutada normalmente de forma automática por el software del verificador y, en todo caso, de acuerdo con la DPC, con los siguientes requisitos:

- a) Es necesario utilizar el software apropiado para la verificación de la firma digital del Certificado Personal de Corporaciones de Derecho Público con los algoritmos y longitudes de claves autorizados en el certificado y/o ejecutar cualquier otra operación criptográfica, y establecer la cadena de certificados en que se basa la firma electrónica a verificar, ya que la firma electrónica se verifica utilizando esta cadena de certificados.
- b) Es necesario asegurar que la cadena de certificados identificada es la más adecuada para la firma electrónica que se verifica, ya que una firma electrónica puede basarse en más de una cadena de certificados, y es decisión del verificador asegurarse de utilizar la cadena más adecuada para verificarla.
- c) Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada en el Depósito de la Entidad de Certificación ANCERT Certificados para Corporaciones de Derecho Público (con CRLs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, pues sólo puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.
- d) Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el poseedor de la clave, debido a la posibilidad de que alguno de los certificados incluyan límites de uso que impidan confiar en la firma electrónica que se verifica. Cada certificado de la cadena dispone de un indicador que hace referencia a las condiciones de uso aplicables, para su revisión por los verificadores.
- e) Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el signatario.

### 3. Diligencia exigible

El verificador tiene que actuar con la máxima diligencia antes de confiar en los certificados. En concreto, el verificador se obliga a utilizar software de verificación de firma electrónica con la capacidad técnica, operativa y de seguridad suficiente para ejecutar el proceso de verificación de firma correctamente, y permanecerá responsable exclusivo del daño que pueda sufrir por la incorrecta elección de dicho software.

La prescripción anterior no será aplicable cuando ANCERT haya suministrado el software de verificación al verificador.

El verificador puede confiar en un certificado si concurren las siguientes condiciones:

- a) La firma electrónica se tiene que poder verificar de acuerdo con los requisitos establecidos en el apartado 4.2.
- b) El verificador tiene que haber utilizado información de revocación actualizada en el momento de verificación de la firma.
- c) El tipo y clase de certificado tiene que ser apropiado para el uso que se pretende hacer.
- d) El verificador ha de tener en cuenta otras limitaciones adicionales de uso del certificado indicadas de cualquier forma en el certificado, incluyendo aquéllas no procesadas automáticamente por el software de verificación, incorporadas por referencia al certificado, y contenidas en estas condiciones de uso. En especial, un certificado no constituye una concesión de derechos y facultades por parte de ANCERT al suscriptor, más allá de la descripción del certificado según la cláusula 3 u otra indicación expresa de ANCERT o del propio suscriptor.
- e) Finalmente, la confianza tiene que ser razonable de acuerdo con las circunstancias. Si las circunstancias requieren garantías adicionales, el verificador tendrá que obtener estas garantías para que la confianza sea razonable.

En cualquier caso, la decisión final con respecto a confiar o no en un certificado verificado es exclusivamente del verificador.

#### 4. Confianza en una firma no verificada

Queda prohibido confiar, o, de cualquier otra manera, hacer uso de una firma o certificado no verificados.

Si el verificador confía en un certificado no verificado, asumirá todos los riesgos derivados de esta actuación.

#### 5. Efecto de la verificación

En virtud de la correcta verificación del Certificado Personal de Corporación de Derecho Público, de conformidad con estas condiciones de uso, el verificador puede confiar en la identificación y, en su caso, clave pública del suscriptor, dentro de las limitaciones de uso correspondientes.

#### 6. Uso correcto y actividades prohibidas

El verificador se obliga a no utilizar ningún tipo de información de estado de los certificados o de ningún otro tipo que haya sido suministrada por ANCERT, en la realización de acto alguno prohibido por la ley aplicable.

El verificador se obliga a no inspeccionar, interferir o realizar ingeniería inversa de la implantación técnica de los servicios públicos de certificación de ANCERT, sin previo consentimiento escrito de ANCERT.

Adicionalmente, el verificador se obliga a no comprometer intencionadamente la seguridad de los servicios públicos de certificación de ANCERT.

Los servicios de certificación digital prestados por ANCERT no han sido diseñados ni permiten la utilización o reventa, como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo, o sistemas de control de armamento, donde un error podría causar la muerte, daños físicos o daños medioambientales graves.

#### **QUINTA. - Obligaciones de ANCERT**

##### 1. Relativas a la prestación del servicio de verificación de certificados

ANCERT se obliga a la prestación del servicio en determinadas condiciones técnicas y operativas, tal como se establece en la DPC, incluyendo un Depósito de certificados, donde se publica información relativa al estado de los certificados.

ANCERT se obliga a emitir información de estado, incluyendo suspensión y revocación, de los certificados emitidos, de acuerdo con la DPC, así como a asumir sus responsabilidades frente a los verificadores, siempre dentro de los límites de uso establecido por los certificados.

##### 2. Garantía limitada de ANCERT

ANCERT garantiza al verificador las siguientes condiciones del servicio:

- a) El certificado contiene información correcta y actual en el momento de su emisión, debidamente comprobada, de conformidad con lo establecido en la Ley 59/2003, de 19 de diciembre.
- b) El certificado cumple todos los requisitos relativos al contenido y al formato establecidos en la DPC.
- c) La clave privada del suscriptor no ha sido comprometida, excepto notificación en contra mediante el Registro.

#### **SEXTA. - Responsabilidad**

##### 1. Responsabilidad del verificador

El verificador responderá por incumplimiento de sus obligaciones contractuales o por negligencia.

El verificador se obliga a mantener a ANCERT indemne de cualquier acto u omisión de la que resulten daños de todo tipo, incluyendo:

- a) El incumplimiento de las obligaciones propias del verificador.

- b) La confianza en un certificado, que no sea razonable.
- c) El incumplimiento de la obligación de comprobar el estado de un certificado para determinar si ha expirado o ha sido suspendido o revocado.

## 2. Responsabilidad de ANCERT

ANCERT responderá por incumplimiento de las obligaciones que, en cada caso, impone la Ley 59/2003, de 19 de diciembre, sobre firma electrónica o por negligencia, excepto en los casos siguientes:

- a) ANCERT no será responsable por los daños causados por las informaciones contenidas en los certificados, siempre que las mismas sean correctas y actuales en el momento de la emisión del certificado.
- b) ANCERT no será responsable de ningún daño directo o indirecto, especial, incidental, emergente, de cualquier lucro cesante, pérdida de datos, daños punitivos, previsibles o imprevisibles, derivados del uso, envío, licencia a terceros, funcionamiento o no funcionamiento de los certificados en un sistema no provisto por ANCERT, así como de las firmas digitales o cualquier otra transacción o servicio descrito en la DPC, cuando sean utilizados fuera del servicio de certificación de ANCERT y de los servicios de verificación de ANCERT.

### **SÉPTIMA.** - *Protección de datos personales*

El verificador reconoce que determinadas informaciones relativas a certificados digitales contienen datos de carácter personal, titularidad de los suscriptores de certificados.

En caso de que el verificador reciba de ANCERT cualquier tipo de información personal en ejecución de las presentes condiciones de uso, se compromete a utilizarla con la finalidad exclusiva de verificar la identidad personal del signatario y las firmas electrónicas de sus mensajes o documentos.

Asimismo, se compromete a proteger los datos personales de conformidad con lo establecido en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, y en especial se obliga al establecimiento de las adecuadas medidas de seguridad, de conformidad con el artículo 9 de la Ley Orgánica 15/1999.

El verificador será responsable exclusivo de las incidencias derivadas de la infracción de estas obligaciones de protección de datos personales, obligándose a mantener indemne a ANCERT de todo daño derivado de estas incidencias.

### **OCTAVA.** - *Infracciones de derechos de terceros*

ANCERT no se responsabiliza de que el envío a ANCERT, por el suscriptor, para su inclusión en el certificado, y la utilización de un dominio y/o otro tipo de nombre o denominación, y el resto de información de solicitud de los certificados, infrinja los derechos de persona alguna en ninguna jurisdicción con respeto a sus marcas registradas, marcas de servicio, nombres comerciales o cualquier otro derecho de propiedad

intelectual o industrial, ni de que el suscriptor pretenda utilizar el dominio y los nombres distinguidos para propósito ilegal alguno, incluyendo, sin limitación, la infracción con dolo de un contrato, o la obtención de posibles ventajas comerciales, la competencia desleal, la lesión del derecho al honor, y la confusión o engaño de una persona, tanto física como jurídica.

ANCERT no se responsabiliza de la legalidad de la información que le haya sido comunicada por el suscriptor, para su inclusión en los certificados emitidos por ANCERT, en ninguna jurisdicción en la que ésta se pueda utilizar o visualizar.

**NOVENA.** - *Divisibilidad de las condiciones de uso*

Las cláusulas de las presentes condiciones de uso son independientes entre sí, motivo por el cual si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas de las presentes condiciones de uso seguirán siendo aplicables, excepto acuerdo expreso contrario de las partes.

**DÉCIMA.** - *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 Depósito 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 las presentes Condiciones Generales de Uso 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.

### **UNDÉCIMA.-** *Limitación de responsabilidades*

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

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

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

### **DUODÉCIMA.** *Divisibilidad de las condiciones de uso*

Las cláusulas de las presentes condiciones de uso son independientes entre sí, motivo por el cual si cualquier cláusula es considerada inválida o inaplicable, el resto de cláusulas de las presentes condiciones de uso seguirán siendo aplicables, excepto acuerdo expreso contrario de las partes

### **DÉCIMOTERCERA.** - *Legislación aplicable y jurisdicción competente*

Las presentes condiciones de uso serán interpretadas y serán ejecutadas en sus propios términos y, en todo aquello no previsto, las partes se regirán para la Ley 59/2003, de 19 de diciembre, por la legislación administrativa aplicable y, subsidiariamente, por la legislación civil y mercantil que regula el régimen de las obligaciones y los contratos.

La jurisdicción competente es la que se indica en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.