

CONDICIONES DE USO

APLICABLES A

CERTIFICADOS CORPORATIVOS DE PERSONA JURÍDICA EN SOFTWARE

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 Registro de la EC-OMC, Usted (en lo sucesivo, "el verificador") debe 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 Registro de la EC-OMC, se entenderá que acepta todas las cláusulas de estas condiciones de uso.

Las condiciones de emisión del certificado corporativo de persona jurídica en software, aplicables al suscriptor o al poseedor de claves del certificado, se hallan reguladas en las "Condiciones Generales de Emisión" aplicables.

En el supuesto de que el Verificador no esté conforme con la totalidad de los términos de las presentes Condiciones de Uso deberá abstenerse de realizar cualquier acción que guarde relación con las cláusulas aquí contenidas. En este caso, EC-OMC no asume responsabilidad alguna

CLÁUSULAS

PRIMERA. - Objeto

1. Estas condiciones de uso regulan la prestación por la OMC de los servicios de información sobre los certificados, el estado de los certificados y otras informaciones publicadas en el Registro, 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 OMC

1. Los Servicios de Certificación de OMC objeto de las presentes condiciones de uso, se regulan técnicamente y operativamente por la Declaración de Prácticas de Certificación de la EC-OMC (en lo sucesivo, la DPC) y sus actualizaciones posteriores, así como por documentación complementaria, publicadas para dar cumplimiento a los artículos 18, y 19 de la Ley 59/2003, sobre firma electrónica, en la siguiente dirección de Internet: <http://www.cgcom.es/registro>

2. La DPC y la documentación de operaciones de la OMC, 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 OMC.

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. - *El certificado corporativo de persona jurídica en software*

1. Descripción del certificado

Este documento da cobertura a los siguientes certificados:

NOMBRE DEL CERTIFICADO	NÚMERO DE OID	FUNCIÓN
Certificados de persona jurídica en software	1.3.6.1.4.1.26852.1.1.5	Identificación, firma y cifrado

Los certificados corporativos de persona jurídica en software de firma electrónica avanzada son certificados reconocidos de acuerdo con lo que se establece en el artículo 7 y 11.1, con el contenido prescrito por el artículo 11.2 y emitidos cumpliendo las obligaciones de los artículos 12, 13, y 17 a 20 de la Ley 59/2003, de 19 de diciembre, de firma electrónica y que dan cumplimiento a lo dispuesto por la normativa técnica del Instituto Europeo de Normas de Telecomunicaciones, identificada con la referencia TS 101 456.

Los certificados corporativos de persona jurídica en software no funcionan necesariamente con dispositivos seguros de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre.

Los certificados corporativos de persona jurídica en software son certificados para el colegio, a emplear en aplicaciones de Administraciones Públicas que expresamente admitan certificados de persona jurídica, y no son emitidos al público en ningún caso. La persona que recibe el certificado de persona jurídica tiene la consideración de poseedor y responsable de custodia de las claves, así como del software complementario correspondiente.

Aunque la firma electrónica avanzada no se equipara directamente a la firma escrita, esta equiparación se puede producir igualmente en virtud de un contrato de firma electrónica o de una norma jurídica específica (por ejemplo la "ORDEN HAC/1181/2003, de 12 de mayo, por la que se establecen normas específicas sobre el uso de la firma electrónica en las relaciones tributarias por medios electrónicos, informáticos y telemáticos con la Agencia Estatal de Administración Tributaria"), que establecerá las condiciones adicionales necesarias para que se produzca dicha equiparación.

Por otra parte, los certificados corporativos de persona jurídica en software se pueden utilizar en otras aplicaciones como las que se indican a continuación:

- a) Autenticación en sistemas de control de acceso.
- b) Firma de correo electrónico seguro.
- c) Otras aplicaciones de firma digital.

Finalmente, los certificados corporativos de persona jurídica en software se pueden utilizar para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado del documento utilizando:

- a) La clave pública del poseedor de claves indicada en el certificado.
- b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública del poseedor de claves indicada en el certificado.

En todo caso, el poseedor de la clave deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y al poseedor de la clave que en ningún caso se podrá recuperar una clave perdida, de forma que la OMC no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

CUARTA.- Licencia de uso del Certificado

1. Reserva de derechos

Todos los contenidos accesibles en relación con la prestación de los servicios de certificación, el propio del certificado corporativo de persona jurídica en software, así como las especificaciones, marcas y demás aplicativos aparejados a su uso están sujetos a derechos de propiedad intelectual e industrial de EC-OMC o de otros terceros titulares de los mismos.

En ningún caso la prestación de dichos servicios implica ningún tipo de renuncia, transmisión o cesión total o parcial de otros derechos que los expresamente reconocidos y otorgados en las presentes Condiciones de Uso.

2. Licencia de uso del certificado corporativo de persona jurídica en software

EC-OMC otorga licencia de uso no exclusiva e intransferible del certificado corporativo de persona jurídica en software y de la información de estado de los mismos al Verificador, con la única y exclusiva finalidad de prestarle los servicios y permitir el uso del certificado de conformidad con las presentes Condiciones de uso.

3. Inexistencia de garantía de idoneidad

EC-OMC no puede garantizar que la utilización del certificado corporativo de persona jurídica en software y aplicativos informáticos aparejados permita al Verificador la obtención o cobertura de necesidades, datos o fines de cualquier índole, distintos a los que pueden ser alcanzados mediante su uso según su propia naturaleza y según lo que se desprende de su licencia de uso.

4. Limitaciones de uso y usos prohibidos

El certificado corporativo de persona jurídica en software sólo podrá ser utilizado dentro de los límites de uso recogidos de manera expresa en su licencia de uso y en las presentes Condiciones de Uso. Cualesquiera otros usos fuera de los descritos en la presente cláusula quedan expresamente excluidos del presente ámbito contractual y formalmente prohibidos.

El certificado no se ha diseñado, no se puede destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieran actuaciones a prueba de errores, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un error pudiera directamente comportar la muerte, lesiones personales o daños medioambientales severos.

5. Duración de la licencia

Los certificados corporativos de persona jurídica en software 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.

QUINTA. - *Obligaciones del verificador*

1. Decisión informada

OMC 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 Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de OMC, se rige por la DPC de la EC-OMC y se compromete a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC de la EC-OMC.

2. Requisitos de verificación de la firma electrónica

Para proceder a cifrar un mensaje o documento por una persona, se ha de utilizar la clave pública del destinatario. Esta clave pública se puede obtener a partir de su certificado corporativo de persona jurídica en software.

Por tanto, es necesario verificar este certificado antes de que se proceda al cifrado.

La comprobación de la firma electrónica del certificado es imprescindible para determinar que la clave pública contenida en el certificado corresponde al poseedor y que la correspondiente clave privada permite descifrar el mensaje.

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 corporativo de persona jurídica en software 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 qué 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 Registro de la EC-OMC (con LRCs, 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.
- f) Determinar la fecha y hora de generación de la firma electrónica, ya que la firma electrónica sólo puede considerarse correctamente verificada si fue creada dentro del periodo de vigencia de la cadena de certificados en que se basa.
- g) Delimitar los datos que han sido firmados digitalmente, ya que los mismos se utilizarán en la verificación de la firma.
- h) Verificar técnicamente la propia firma con el certificado del signatario avalado por la cadena de certificados.

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 la EC-OMC 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 que se encuentren 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 OMC al suscriptor o al poseedor de claves, más allá de la descripción del certificado según la cláusula 3.1 u otra indicación expresa de la EC-OMC 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, quien debe adoptar una actitud activa y al que se le exige el acceso a toda la información dispuesta por EC-OMC para tomar sus decisiones de forma totalmente informada. En caso de duda, el Verificador no deberá confiar en el certificado corporativo de persona jurídica en software.

4. Confianza en una firma no verificada

Queda prohibido cifrar mensajes o documentos por un destinatario sin haber verificado con éxito su certificado.

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 corporativo de persona jurídica en software, de conformidad con estas condiciones de uso, el verificador puede confiar en la identificación y, en su caso, clave pública del poseedor de claves, 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 la EC-OMC, 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 la EC-OMC, sin previo consentimiento escrito de la EC-OMC.

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

Los servicios de certificación digital prestados por la EC-OMC 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.

SEXTA. - Obligaciones de la EC-OMC

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

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

La EC-OMC 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 la EC-OMC

La EC-OMC 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 que se encuentran establecidos en la DPC.
- c) La clave privada de la EC-OMC no ha sido comprometida, excepto notificación en contra mediante el Registro.

SÉPTIMA. - Responsabilidad

1. Responsabilidad del verificador

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

El verificador se obliga a mantener a la EC-OMC 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 la EC-OMC

La EC-OMC 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) La EC-OMC 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) La EC-OMC 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 la EC-OMC, 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 la EC-OMC y los servicios de verificación de la EC-OMC.

OCTAVA. - *Protección de datos personales*

El verificador reconoce que determinadas informaciones relativas a certificados digitales contienen datos de carácter personal, titularidad de los poseedores de claves y, en su caso, de los suscriptores de certificados.

En caso de que el verificador reciba de la EC-OMC 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, y normativa de desarrollo.

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 la EC-OMC de todo daño derivado de estas incidencias.

NOVENA. - *Infracciones de derechos de terceros*

La EC-OMC no se responsabiliza de que el envío a la EC-OMC, por el suscriptor o por el poseedor de claves, 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 o el poseedor de claves 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.

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

DÉCIMA. - *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 en contrario de las partes.

DÉCIMO PRIMERA. - *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 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.