

CONDICIONES GENERALES DE CONTRATACIÓN



Condiciones generales de contratación del servicio de certificación corporativa

PRIMERA. Objeto y documentación de los servicios de certificación

Estas condiciones generales regulan los servicios de certificación del Consejo General de Colegios de Médicos de España (en lo sucesivo, CGCOM) al colegio solicitante de servicios, que se convierte en suscriptor de los certificados, identificado en el convenio de prestación del servicio.

Las condiciones generales regulan las cláusulas de aplicación común a todos los colegios suscriptores de los servicios de certificación, en atención al carácter común y compartido de la Entidad de Certificación, mientras que el convenio de prestación del servicio regula las opciones particulares de cada colegio.

Los servicios de certificación de CGCOM se regulan técnicamente y operativamente por la Declaración de prácticas de certificación de la Entidad de Certificación de CGCOM (en lo sucesivo, DPC) y por sus actualizaciones posteriores, así como por documentación complementaria suministrada al colegio.

La DPC y la documentación de operaciones de CGCOM, que se modifican según se indica periódicamente en el Registro de certificación, consultables en la página <https://www.cgcom.es/certificacion>, se incorporan a estas condiciones generales por referencia. En caso de discrepancia, el significado de los términos contenidos en estas condiciones generales prevalecerá respecto del que se establece en la DPC.

SEGUNDA. Características de los certificados

2.1. Certificado corporativo de colegiado

Los certificados corporativos de colegiado son certificados reconocidos de conformidad con lo que se establece en el artículo 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.

Los certificados corporativos de colegiado funcionan con un dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19

de diciembre, y 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 se emiten a colegiados del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este colegiado tiene la consideración de poseedor de claves y de la tarjeta, y del software complementario correspondientes.

Los certificados corporativos de colegiado garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Asimismo garantizan la condición de colegiado, dada la intervención obligatoria del colegio en el procedimiento de emisión del certificado, actuando como entidad de registro o como garante de la información.



Por otra parte, los certificados corporativos de colegiado se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del suscriptor, como las aplicaciones 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.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

Finalmente, los certificados corporativos de colegiado 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 CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

Los certificados corporativos de colegiado se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.26852.1.1.1.

2.2. Certificado corporativo de órgano colegial

Los certificados corporativos de órgano colegial son certificados reconocidos de acuerdo con lo que se establece en el artículo 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.

Los certificados corporativos de órgano colegial funcionan con un dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y 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 se emiten a órganos colegiales del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este órgano tiene la consideración de poseedor de claves y de la tarjeta y el software complementario correspondientes.

Los certificados corporativos de órgano colegial garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Asimismo, incluyen una manifestación relativa a la categoría y el cargo orgánico del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos. Es necesario advertir que esta indicación no es, por sí sola, suficiente por determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por lo tanto, el usuario del certificado tendrá que comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes al certificado, como por ejemplo, el servicio de validación del CGCOM.

Por otra parte, los certificados corporativos de órgano colegial pueden ser utilizados en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del suscriptor, como las aplicaciones 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.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

Finalmente, los certificados corporativos de órgano colegial 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 CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

Los certificados corporativos de órgano colegial se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.26852.1.1.4.

2.3. Certificado corporativo de personal administrativo

Los certificados corporativos de personal administrativo son certificados reconocidos de acuerdo con lo que se establece en el artículo 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.

Los certificados corporativos de personal administrativo funcionan con un dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y 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 se emiten a personal administrativo del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso. Este órgano tiene la consideración de poseedor de claves y de la tarjeta y el software complementario correspondientes.

Los certificados corporativos de personal administrativo garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Asimismo, incluyen una manifestación relativa a la categoría del poseedor de claves, que han sido comprobados antes de emitir el certificado, y son correctos. Es necesario advertir que esta indicación no es, por sí sola, suficiente por determinar las facultades que tiene el poseedor de claves para firmar en nombre del suscriptor; por lo tanto, el usuario del certificado tendrá que comprobar las facultades y poderes de firma del poseedor mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación del CGCOM.

Por otra parte, los certificados corporativos de personal administrativo se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del suscriptor, como las aplicaciones 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.

La firma electrónica generada en el uso de estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

Finalmente, los certificados corporativos de personal administrativo 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 CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

Los certificados corporativos de órgano colegial se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.26852.1.1.2.

2.4. Certificado corporativo de colegio profesional

Los certificados corporativos de colegio profesional 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.

Los certificados corporativos de colegio profesional funcionan con dispositivo seguro de creación de firma electrónica, de acuerdo con el artículo 24.3 de la Ley 59/2003, de 19 de diciembre, y 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 colegio profesional 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 colegio profesional tiene la consideración de poseedor y responsable de custodia de las claves, así como de la tarjeta y el software complementario correspondientes.

Los certificados corporativos de colegio profesional garantizan la identidad del suscriptor y del poseedor de la clave privada de identificación y firma, y permiten la generación de la "firma electrónica reconocida"; es decir, la firma electrónica avanzada que se basa en un certificado reconocido y que ha sido generada empleando un dispositivo seguro, por lo cual, de acuerdo con lo que establece el artículo 3 de la Ley 59/2003, de 19 de diciembre, se equipara a la firma escrita por efecto legal, sin necesidad de cumplir ningún otro requisito adicional.

Por otra parte, los certificados corporativos de colegio profesional se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, sino sólo la identificación del poseedor de claves, en nombre del suscriptor, como las aplicaciones 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.

La firma electrónica generada usando estas aplicaciones tendrá los efectos que determine la normativa reguladora de la aplicación, que podrá declarar la equivalencia con la firma escrita o sólo el efecto de identificación, puesto que, cuando menos, esta firma habrá sido producida con el dispositivo seguro.

Finalmente, los certificados corporativos de personal administrativo 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 CGCOM no responderá por ninguna pérdida de información cifrada que no se pueda recuperar en casos de pérdida de certificados o claves.

Los certificados corporativos de colegio profesional se identifican con el identificador de objeto (OID): 1.3.6.1.4.1.26852.1.1.3.

2.5. Duración de los certificados

Todos los certificados emitidos de acuerdo con este convenio tendrán un periodo máximo de validez de tres años desde el día en que sean emitidos.

La fecha de expiración de los certificados figura indicada dentro los mismos certificados.

TERCERA. Obligaciones del suscriptor

3.1. Solicitud del servicio y generación de las claves

El suscriptor solicitará y autorizará a CGCOM que genere las claves del suscriptor, privada y pública, correspondientes a las funcionalidades de identificación, firma y cifrado, dentro de un dispositivo seguro de creación de firma electrónica (la tarjeta colegial que recibe el poseedor de claves), y realice la emisión del certificado correspondiente.

El suscriptor podrá actuar como entidad de registro, solicitando a CGCOM que le provea los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de tarjetas colegiales, mediante la firma de un protocolo adicional a las presentes condiciones generales.

3.2. Personal responsable de la ejecución de los procedimientos

El suscriptor se obliga a nombrar frente a CGCOM a las siguientes personas:

a) Una o más personas a su servicio, denominadas "responsables del servicio", que actuarán como interlocutores con CGCOM en todo aquello referido a los servicios de certificación.

b) Una o más personas a su servicio, denominadas "solicitantes", para realizar las solicitudes de emisión, suspensión, alzamiento de la suspensión, revocación y renovación

de los certificados, de acuerdo con los procedimientos suministrados por CGCOM.

c) Una o más personas a su servicio, denominadas "certificadores", para aportar la justificación documental necesaria para el registro de usuarios por CGCOM y la posterior emisión de certificados.

3.3. Veracidad de la información

El suscriptor se responsabilizará de que toda la información incluida, por cualquier medio, en la solicitud del certificado y en el mismo certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor puede delegar completamente en CGCOM, delegación sometida a aceptación expresa posterior, la ejecución y la responsabilidad asociada a las funciones de entidad de registro de los certificados.

El suscriptor debe informar inmediatamente a CGCOM de cualquier inexactitud en el certificado, detectada una vez se haya emitido, así como de los cambios que se produzcan en la información aportada por el suscriptor para la emisión del certificado.

En el supuesto de que un poseedor de claves a quien se haya emitido un certificado cese en su vinculación con el suscriptor, dicho suscriptor debe solicitar inmediatamente la revocación del certificado.

3.4. Entrega y aceptación del servicio

El suscriptor queda vinculado y acepta el servicio desde la solicitud del mismo.

Por su parte, en virtud de la entrega de la tarjeta y de la recepción de las claves de uso y de la hoja de entrega, el poseedor de claves acepta el certificado, quedando vinculado por las condiciones de uso del certificado correspondiente.

3.5. Poseedores de claves del suscriptor

El suscriptor se obliga a informar los poseedores de claves de los términos y condiciones relativos al uso de los certificados, así como de los procedimientos internos de gestión de certificados que pueda establecer adicionalmente a los provistos por CGCOM.

3.6. Obligaciones de custodia

El suscriptor se obliga a custodiar, cuando sea preciso, el código de identificación personal, la tarjeta o cualquier otro elemento técnico entregado por CGCOM, las claves privadas y, dado el caso, las especificaciones propiedad de CGCOM que le fuesen suministradas, así como toda la información que genere en su actividad como entidad de registro.

En caso de pérdida o robo de la clave privada del certificado, o en caso de que el suscriptor sospeche que la clave privada ha perdido fiabilidad por cualquier motivo, debe notificarlo inmediatamente a CGCOM.

3.7. Obligaciones de uso correcto

El suscriptor debe utilizar el servicio de certificación prestado por CGCOM exclusivamente para los usos autorizados en la DPC, excepto declaración expresa y por escrito en otro sentido realizada por CGCOM.

El suscriptor se obliga a utilizar el servicio de certificación digital, la pareja clave pública/clave privada, la tarjeta y cualquier otro elemento técnico entregado por CGCOM y los certificados, de acuerdo con estas condiciones generales, las condiciones particulares que en su caso resulten aplicables, y con cualquier otra instrucción, manual o procedimiento suministrados por CGCOM al suscriptor.

3.8. Transacciones prohibidas

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

CUARTA. Obligaciones de CGCOM

4.1. Prestación del servicio de entidad de registro

CGCOM se obliga al registro de los datos del certificado y a su emisión posterior al suscriptor, para lo cual debe realizar las comprobaciones que considere oportunas respecto de la identidad y otras informaciones personales y complementarias de los suscriptores y, cuando resulte procedente, de los poseedores de claves.

Estas comprobaciones deben incluir la justificación documental aportada por el suscriptor y, si CGCOM lo considera necesario, cualquier otro documento e información relevantes, facilitados por el suscriptor, por el poseedor de claves, o por terceras personas.

En el caso que CGCOM detecte errores en los datos que se deben incluir en los certificados o que justifican estos datos, podrá realizar los cambios que considere necesarios antes de emitir el certificado o suspender el proceso de emisión y gestionar con el suscriptor la incidencia correspondiente. En caso de que CGCOM corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

CGCOM se reserva el derecho a no emitir el certificado, cuando la justificación documental aportada resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del poseedor de claves.

Las anteriores obligaciones quedarán en suspenso en los casos en que el suscriptor actúe como entidad de registro y disponga de los elementos técnicos correspondientes a la generación de claves, emisión de certificados y grabación de tarjetas colegiales.

4.2. Prestación del servicio de certificación digital

CGCOM se obliga a:

- a) Emitir, entregar, administrar, suspender, revocar y renovar certificados, de acuerdo con las instrucciones suministradas por el suscriptor, en los casos y por los motivos descritos en la DPC de CGCOM.
- b) Ejecutar los servicios con los medios técnicos y materiales adecuados, y con personal que cumpla las condiciones de cualificación y experiencia establecidas en la DPC.
- c) Cumplir los niveles de calidad del servicio, en conformidad con lo que se establece en la DPC, en los aspectos técnicos, operativos y de seguridad.

- d) Notificar al suscriptor, como mínimo con dos meses de antelación a la fecha de expiración de los certificados y la posibilidad de renovarlos, así como la suspensión, alzamiento de esta suspensión o revocación de los certificados, cuando se produzcan dichas circunstancias.
- e) Comunicar a las terceras personas que lo soliciten, el estado de los certificados, de acuerdo con lo que se establece en la DPC para los diferentes servicios de verificación de certificados.

QUINTA. Garantías

5.1. Garantía de CGCOM por los servicios de certificación digital

CGCOM garantiza que la clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a no ser que haya comunicado lo contrario mediante el registro de certificación, de acuerdo con la DPC.

CGCOM únicamente garantiza al suscriptor, en el momento de la emisión del certificado, que:

- a) Los certificados son reconocidos y funcionan en dispositivo seguro de creación de firma, en los términos previstos en la Ley 59/2003, de 19 de diciembre.
- b) CGCOM no ha originado ni ha introducido declaraciones falsas o erróneas en la información de certificado alguno, ni ha dejado de incluir información necesaria aportada y verificada por el suscriptor.
- c) Todos los certificados cumplen los requisitos formales y de contenido previstos en la DPC de CGCOM.
- d) CGCOM ha cumplido los procedimientos descritos en la DPC.

CGCOM aplica una diligencia razonable para asegurar que cada producto suministrado en la prestación de sus servicios se encuentra libre de virus informático, gusanos y otros códigos ilícitos, y se obliga a comunicar al suscriptor cualquier virus, gusano u otros códigos ilícitos descubiertos posteriormente en cualquier producto.

5.2. Exclusiones de la garantía

CGCOM no garantiza software alguno que utilice el suscriptor de certificados o el poseedor de claves, o cualquier otra persona, para generar, verificar o utilizar de otra forma firma digital o certificado digital alguno emitido por CGCOM, excepto cuando exista una declaración escrita de CGCOM en sentido contrario.

SEXTA. Responsabilidad del suscriptor

El suscriptor debe responder ante cualquier persona por el incumplimiento de sus obligaciones y, en especial, de la actividad como entidad de registro, según los términos de estas condiciones generales.

El suscriptor es responsable de todas las comunicaciones electrónicas autenticadas mediante una firma digital generada con su clave privada, cuando el certificado haya sido válidamente verificado mediante los mecanismos y las condiciones establecidos por CGCOM.

Mientras no se produzca la notificación establecida en el apartado 3.6 de estas condiciones generales, la responsabilidad que se pueda derivar del uso no autorizado y/o indebido de los certificados corresponde, en todo caso, al suscriptor.

SÉPTIMA. Responsabilidad de CGCOM

7.1. Responsabilidad como prestador de servicios de certificación

CGCOM responde ante el suscriptor y cualquier tercera persona por el incumplimiento de las obligaciones legalmente impuestas por la Ley 59/2003, de 19 de diciembre, y según los términos de estas condiciones generales.

CGCOM no será responsable:

- a) En los casos previstos en el artículo 23 de la Ley 59/2003, de 19 de diciembre, de firma electrónica.
- b) De las informaciones contenidas en los certificados, siempre que su contenido cumpla estas condiciones generales y la DPC.
- c) De ningún daño directo o indirecto, especial, incidental o emergente; de ningún lucro cesante, pérdida de datos, daños morales o punitivos, previsibles o imprevisibles derivados del uso, distribución, licencia, funcionamiento de los certificados, las firmas digitales o cualquier transacción basada en certificados digitales, incluso aunque CGCOM hubiera sido advertido de la posibilidad de la producción de los daños.

7.2. Adecuación de los productos que hacen uso de la identificación, la firma electrónica o el cifrado

CGCOM no se hace responsable de la adecuación de los productos y servicios relacionados con la certificación digital, la identificación, la firma electrónica o el cifrado existentes en el mercado que sean utilizados en aplicaciones informáticas del suscriptor, excepto cuando CGCOM los suministre. En este caso, las partes quedarán sujetas a las correspondientes condiciones de uso.

OCTAVA. Lugar de prestación de la actividad

El lugar de cumplimiento de las obligaciones de CGCOM relativas a los servicios de certificación digital y, en su caso, licencias de uso de software es el domicilio de CGCOM en Plaza de las Cortes, 11, 28014 Madrid.

NOVENA. Licencia de software

CGCOM concede al suscriptor, con carácter no exclusivo e intransferible, licencia para utilizar las copias del software recibido de CGCOM para la operación de la tarjeta, así como para la producción de la firma electrónica y los restantes servicios criptográficos por parte de los poseedores de claves.

El suscriptor puede hacer copias del software únicamente con el fin de archivo o copia de seguridad.

En caso de que cualquier persona diferente de CGCOM haga modificaciones en el software suministrado, todas las garantías respecto al software quedarán inmediatamente canceladas.

DÉCIMA. Propiedad de los certificados y las tarjetas

Los certificados y las tarjetas de los suscriptores suministradas permanecen propiedad de CGCOM, que se reserva el derecho discrecional de retirar o sustituir las tarjetas con certificados emitidos, por razones de seguridad, cuando queden obsoletas tecnológicamente o por cualquier otro motivo justificado.

UNDÉCIMA. Condiciones económicas del servicio

El importe de los servicios de certificación del CGCOM se fija en 12 € por carné y certificado emitido cuya validez es de tres años. Dicha cantidad será abonada en el plazo de 30 días desde la recepción del carné.

Pasado este periodo de 3 años, el certificado caduca y la renovación del servicio quedará sujeta a las condiciones económicas que se fijen en función de la evolución del mercado.

DUODÉCIMA. Uso de la imagen corporativa de las partes

Las partes se conceden mutuamente, con carácter no exclusivo e intransferible, una licencia de uso de los diferentes elementos de su imagen corporativa, incluyendo los signos distintivos, logotipos y marcas registradas por cada parte, exclusivamente en los materiales de marketing, publicidad, hojas de información de productos y servicios, paquetes de productos y servicios, páginas web que utilicen los productos y servicios de las partes, así como en las tarjetas y documentación empleadas en los procedimientos de certificación.

El uso de los elementos de la imagen corporativa de cada parte se ha de ajustar, en todo momento, al manual de imagen corporativa correspondiente, así como a las instrucciones de cada parte.

Ninguna parte concede a la otra parte derecho alguno sobre la marca registrada, el nombre comercial, el nombre de la empresa o las buenas prácticas comerciales de cada parte, excepto los derechos que se concretan en estas condiciones generales.

Ninguna parte puede eliminar ni destruir indicación alguna relativa a los derechos de autor, las patentes o las marcas comerciales contenidos en cualquier producto, servicio electrónico o documentación de todo tipo.

DECIMOTERCERA. Protección de los datos personales

CGCOM es titular de un conjunto de ficheros de datos de carácter personal relativos a los datos de identificación y autenticación de los usuarios de los servicios de certificación digital, tal y como se especifica en la DPC.

CGCOM obtiene los datos personales que figuran en los ficheros por varios procedimientos:

- a) Por cesión de los datos por parte del suscriptor, que debe haberlos obtenido legalmente, en las condiciones previstas en la normativa sobre firma electrónica y sobre protección de datos de carácter personal.
- b) Directamente de los poseedores de claves, cuando el registro de sus datos es efectuado por CGCOM.

CGCOM se obliga a cumplir la normativa sobre firma electrónica y sobre protección de datos de carácter personal, en especial con respecto a la inscripción y la correcta gestión de los ficheros de datos personales, con las medidas de seguridad correspondientes según se relaciona en la Ley Orgánica 15/1999 de Protección de Datos Personales, y en el Real Decreto 1720/2007 de desarrollo de la citada Ley.

El suscriptor queda liberado de cualquier responsabilidad derivada del daño ocasionado por las incidencias producidas por la gestión de los datos de carácter personal cedidos a CGCOM.

DECIMOCUARTA. Divisibilidad de las Condiciones Generales

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

DECIMOQUINTA. Resolución

La resolución tendrá lugar en los casos siguientes:

- a) Por incumplimiento por la otra parte, de cualquiera de sus obligaciones, si esta infracción no ha sido solucionada:
 - a. Dentro de los treinta días desde la recepción de la notificación efectuada por la parte que no ha dejado de cumplir sus obligaciones.
 - b. Inmediatamente, si el incumplimiento compromete la seguridad de los servicios.

b) Por concurrencia de cualquier otra causa de resolución anticipada establecida por la legislación vigente y, especialmente, por la legislación vigente de firma electrónica y certificación digital.

DECIMOSEXTA. Legislación aplicable y jurisdicción competente

Las presentes Condiciones Generales serán interpretadas y ejecutadas en sus propios términos y, en todo aquello no previsto, las partes se regirán por la Ley 59/2003, de 19 de diciembre 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 6/1985, de 1 de julio, del Poder Judicial.

