OMC
ORGANIZACIÓN MÉDICA COLEGIAL DE ESPAÑA | CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS

Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780
cgcom@cgcom.es
www.cgcom.es

TEXTO DIVULGATIVO - PDS

1. INFORMACIÓN GENERAL

Estado formal		
Preparado por:	**Revisado por:**	**Aprobado por:**
Nombre: VH Fecha: 10-01-2020	Nombre: Fecha:	Nombre: Fecha:

Control de versiones				
Versión	**Partes que cambian**	**Descripción del cambio**	**Autor del cambio**	**Fecha del cambio**
2.0	Original		VH	10-01-2020
2.1		Adaptación Ley 6/2020	Astrea	12-05-2021
2.2	2.1.3, 2.2.1, 2.3	Ampliación perfiles Correcciones menores	Astrea	23-03-2022
2.3		Revisión anual	Astrea	10-05-2023

Índice

1. INFORMACIÓN GENERAL 2
1. Información de contacto 5
1.1. Organización responsable 5
1.2. Organización que administra el documento 5
1.3. Persona de contacto 5
1.4. Contacto para procesos de revocación 5
2. Tipo y finalidad del certificado 6
2.1. Certificados cualificados de persona física 6
2.1.1. Certificados en tarjeta 6
2.1.2. Certificados en NUBE 6
2.1.3. Certificados en software 6
2.1.4. Certificados para identificación 7
2.1.5. Certificados para firma 7
2.1.6. Certificados para cifrado 7
2.1.7. Certificados de médico colegiado 7
2.1.8. Certificados de Representante de Persona Jurídica 8
2.1.9. Certificado de Persona Física Vinculada a una Organización 8
2.2. Certificados cualificados de sello electrónico 8
2.2.1. Certificados de sello cualificado en NUBE 8
2.2.1. Certificados de sello cualificado en software 8
2.3. Tipos de certificados 9
2.4. Entidad de Certificación emisora 10
2.5. Validación de los certificados 10
3. Límites de uso del certificado 11
3.1. Límites de uso dirigidos a los firmantes 11
3.2. Límites de uso dirigidos a los verificadores 11
4. Obligaciones de los suscriptores 12
4.1. Generación de claves 12
4.2. Solicitud de certificados 12
4.3. Veracidad de la información 13
4.4. Obligaciones de custodia 13
5. Obligaciones de los firmantes y creadores de sellos 13

5.1. Obligaciones de custodia 13
5.2. Obligaciones de uso correcto 13
5.3. Transacciones prohibidas....14
6. Obligaciones de los verificadores 14
6.1. Decisión informada....14
6.2. Requisitos de verificación de la firma electrónica 15
6.3. Confianza en un certificado no verificado....16
6.4. Efecto de la verificación 16
6.5. Uso correcto y actividades prohibidas 16
6.6. Cláusula de indemnidad....16
7. Obligaciones de la AC-CGCOM 17
7.1. En relación con la prestación del servicio de certificación digital 17
7.2. En relación con las comprobaciones del registro 17
8. Garantías limitadas y rechazo de garantías.... 18
8.1. Garantía de la AC-CGCOM por los servicios de certificación digital 18
8.2. Exclusión de la garantía 19
9. Acuerdos aplicables y DPC 19
9.1. Acuerdos aplicables 19
9.2. Declaración de prácticas de certificación 20
9.3. Política de certificación 20
10. Reglas de confianza para firmas longevas 20
11. Política de intimidad 20
12. Política de privacidad 21
13. Política de reintegro.... 21
14. Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas 22
15. Acreditaciones 22
16. Vinculación con la lista de prestadores.... 22
17. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación 23

1. Información de contacto

1.1. Organización responsable

La Autoridad de Certificación del "Consejo General de Colegios Oficiales de Médicos", en lo sucesivo "AC-CGCOM", es una iniciativa de:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS PLAZA DE LAS CORTES, 11- 28014 MADRID TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.2. Organización que administra el documento

COMISIÓN PERMANENTE DEL CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS PLAZA DE LAS CORTES, 11- 28014 MADRID TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.3. Persona de contacto

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS PLAZA DE LAS CORTES, 11- 28014 MADRID TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

1.4. Contacto para procesos de revocación

Para los procesos de revocación, diríjanse a:

CONSEJO GENERAL DE COLEGIOS OFICIALES DE MÉDICOS

· UNIDAD TECNOLÓGICA ·

PLAZA DE LAS CORTES, 11- 28014 MADRID

TELÉFONO: 91 431 77 80 / FAX: 91 576 43 88

2. Tipo y finalidad del certificado

2.1. Certificados cualificados de persona física

Estos certificados son cualificados de acuerdo con el artículo 28 y con el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

2.1.1. Certificados en tarjeta

Los certificados que usan tarjeta funcionan con dispositivo cualificado de creación de firma electrónica, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

2.1.2. Certificados en NUBE

Estos certificados son gestionados de forma centralizada.

Estos certificados funcionan con dispositivo cualificado de creación de firma, de acuerdo con el Anexo II del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado, y permiten la generación de la “firma electrónica cualificada basada en certificado electrónico cualificado”.

2.1.3. Certificados en software

Estos certificados son gestionados en ubicaciones locales del usuario.

Estos certificados no funcionan con dispositivos cualificados de creación de firma.

Estos certificados garantizan la identidad del suscriptor y de la persona indicada en el certificado.

2.1.4. Certificados para identificación

Los certificados con la función de identificación garantizan la identidad del subscriptor y del firmante.

2.1.5. Certificados para firma

Los certificados con la función de firma permiten la generación de la "**firma electrónica cualificada**"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado cuando haya sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

2.1.6. Certificados para cifrado

Los certificados con la función de cifrado pueden utilizarse para cifrar documentos propios o para recibir documentos confidenciales, en cualquier formato, protegidos mediante el cifrado utilizando:

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

En todo caso, se deberá utilizar la clave privada para descifrar el mensaje, advirtiéndose al suscriptor del certificado y a la persona indicada en el certificado 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.**

2.1.7. Certificados de médico colegiado

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 firmante.
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.

2.1.8. Certificados de Representante de Persona Jurídica

Estos certificados garantizan la identidad del suscriptor y del firmante, y una relación de representación legal o apoderamiento general entre el firmante y una entidad, colegio de médicos u organización del ámbito sanitario, descrita en el campo "O" (Organization).

Asimismo, incluyen una manifestación relativa a la categoría del firmante, que ha sido comprobada antes de emitir el certificado, y es correcta. Es necesario advertir que esta indicación no es, por si sola, suficiente por determinar las facultades que tiene el firmante para firmar, en su caso, en nombre del suscriptor del servicio de certificación; por lo tanto, la parte usuaria tendrá que comprobar las facultades y poderes de firma del firmante mediante otros medios, diferentes al certificado, como por ejemplo el servicio de validación de CGCOM.

2.1.9. Certificado de Persona Física Vinculada a una Organización

Los certificados se emiten a personas físicas vinculadas del ámbito corporativo del colegio suscriptor o de la persona jurídica del ámbito sanitario, y no son emitidos al público en ningún caso. Esta persona tiene la consideración de firmante y, en su consecuencia, de poseedor de la tarjeta y el software complementario correspondientes.

2.2. Certificados cualificados de sello electrónico

Estos certificados son cualificados de acuerdo con el artículo 38 y con el Anexo III del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 y dan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-2.

2.2.1. Certificados de sello cualificado en NUBE

Los certificados de sello electrónico permiten la generación de la "firma electrónica cualificada"; es decir, la firma electrónica avanzada que se basa en un certificado cualificado y que ha sido generada empleando un dispositivo cualificado, por lo cual, de acuerdo con lo que establece el artículo 25.2 del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, tendrá un efecto jurídico equivalente al de una firma manuscrita.

2.2.1. Certificados de sello cualificado en software

Estos certificados son gestionados en ubicaciones locales del creador de sellos.

Estos certificados no funcionan con dispositivos cualificados de creación de firma.

Estos certificados se emiten a Colegios de Médicos y personas jurídicas del ámbito sanitario, y no son emitidos al público en ningún caso.

2.3. Tipos de certificados

Tipo	Soporte	Usos	OID
De Médico Colegiado	Tarjeta	Autenticación	• 1.3.6.1.4.1.26852.1.1.1.1 • 0.4.0.2042.1.2
		Firma	• 1.3.6.1.4.1.26852.1.1.1.2 • 0.4.0.194112.1.2
		Cifrado	• 1.3.6.1.4.1.26852.1.1.1.3
	Centralizado en NUBE	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.1.4 • 0.4.0.194112.1.2
	En software	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.1.5 • 0.4.0.194112.1.0

Tipo	Soporte	Usos	OID
De Persona Física Vinculada	Tarjeta	Autenticación	• 1.3.6.1.4.1.26852.1.1.2.1 • 0.4.0.2042.1.2
		Firma	• 1.3.6.1.4.1.26852.1.1.2.2 • 0.4.0.194112.1.2
		Cifrado	• 1.3.6.1.4.1.26852.1.1.2.3
	Centralizado en NUBE	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.6 • 0.4.0.194112.1.2
	En software	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.2.5 • 0.4.0.194112.1.0

Tipo	Soporte	Usos	OID
De Representante Legal	Tarjeta	Autenticación	• 1.3.6.1.4.1.26852.1.1.11.1 • 0.4.0.2042.1.2 • 2.16.724.1.3.5.8
		Firma	• 1.3.6.1.4.1.26852.1.1.11.2 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.8
		Cifrado	• 1.3.6.1.4.1.26852.1.1.11.3 • 2.16.724.1.3.5.8
	Centralizado en NUBE	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.12 • 0.4.0.194112.1.2 • 2.16.724.1.3.5.8
	En software	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.11.5 • 0.4.0.194112.1.0 • 2.16.724.1.3.5.8

Tipo	Soporte	Usos	OID
De Sello electrónico de persona jurídica	Centralizado en NUBE	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.10.2 • 0.4.0.194112.1.3
	En software	Autenticación, Firma	• 1.3.6.1.4.1.26852.1.1.10.5 • 0.4.0.194112.1.1

2.4. Entidad de Certificación emisora

Estos certificados son emitidos por la Autoridad de Certificación del CGCOM (AC-CGCOM), identificada mediante los datos indicados anteriormente.
La AC-CGCOM subcontrata los servicios de producción de certificados a la empresa Vintegris, como proveedor técnico, que siempre actúa siguiendo las indicaciones de la AC-CGCOM.

2.5. Validación de los certificados

Las listas de certificados revocados y servicios OCSP se encuentran en la web de la AC-CGCOM y en las URL indicadas en cada uno de los certificados.

3. Límites de uso del certificado

3.1. Límites de uso dirigidos a los firmantes

El firmante y el creador de sellos han de utilizar el servicio de certificación prestado por la AC-CGCOM exclusivamente para los usos autorizados en el convenio firmado entre el CGCOM y el colegio o la persona jurídica suscriptora, y que se reproducen posteriormente.

Asimismo, el firmante y el creador de sellos se obligan a utilizar el servicio de certificación digital de acuerdo con las instrucciones, manuales o procedimientos suministrados por la AC-CGCOM.

El firmante y el creador de sellos han de cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas que emplee.

El firmante y el creador de sellos no pueden adoptar medidas de inspección, alteración o ingeniería inversa de los servicios de certificación digital de la AC-CGCOM, sin previo permiso expreso.

3.2. Límites de uso dirigidos a los verificadores

Los certificados se emplean para su función propia y finalidad establecida, sin que puedan emplearse en otras funciones y con otras finalidades.

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

Los certificados no pueden emplearse para firmar peticiones de emisión, renovación, suspensión o revocación de certificados, ni para firmar certificados de clave pública de ningún tipo, ni firmar listas de revocación de certificados (LRC).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa como equipos de control de situaciones peligrosas o para usos que requieren actuaciones a prueba de fallos, como el funcionamiento de instalaciones nucleares, sistemas de navegación o comunicaciones aéreas, o sistemas de control de armamento, donde un fallo pudiera directamente conllevar la muerte, lesiones personales o daños medioambientales severos. Se deben tener en cuenta los límites indicados en los diversos campos de los perfiles de certificados, visibles en el web de la CGCOM https://psc.cgcom.es

El empleo de los certificados digitales en operaciones que contravienen este texto de divulgación (PDS), o los contratos con los suscriptores, tiene la consideración de uso indebido a los efectos legales oportunos, eximiéndose por tanto a la AC-CGCOM, en función de la legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

La AC-CGCOM no tiene acceso a los datos sobre los que se puede aplicar el uso de un certificado. Por lo tanto, y como consecuencia de esta imposibilidad técnica de acceder al contenido del mensaje, no es posible por parte de la AC-CGCOM emitir valoración alguna sobre dicho contenido, asumiendo por tanto el suscriptor, el firmante o la persona responsable de la custodia, cualquier responsabilidad dimanante del contenido aparejado al uso de un certificado.

Asimismo, le será imputable al suscriptor o al firmante cualquier responsabilidad que pudiese derivarse de la utilización de este fuera de los límites y condiciones de uso recogidas en este texto de divulgación, o en los contratos con los suscriptores, así como de cualquier otro uso indebido del mismo derivado de este apartado o que pueda ser interpretado como tal en función de la legislación vigente.

4. Obligaciones de los suscriptores

4.1. Generación de claves

En los certificados en tarjeta, el suscriptor autoriza al firmante a generar sus claves privada y pública dentro de un dispositivo cualificado de creación de firma electrónica, y solicita, en nombre del firmante, la emisión del certificado a la AC-CGCOM.

En los certificados en NUBE, el suscriptor autoriza al firmante a generar sus claves privada y pública, y solicita, en nombre del firmante, la emisión del certificado a la AC-CGCOM.

En los certificados de sello electrónico, el suscriptor autoriza a AC-CGCOM a generar las claves, privada y pública, para su uso por los creadores de sellos, y solicita en su nombre la emisión del certificado de sello electrónico.

4.2. Solicitud de certificados

El suscriptor se obliga a realizar las solicitudes de certificados de acuerdo con el procedimiento y, si es necesario, los componentes técnicos suministrados

por la AC-CGCOM, de conformidad con lo que se establece en la DPC y en la documentación de operaciones de la AC-CGCOM.

4.3. Veracidad de la información

El suscriptor se responsabiliza de que toda la información incluida en su solicitud del certificado sea exacta, completa para la finalidad del certificado y esté actualizada en todo momento.

El suscriptor tiene que informar inmediatamente a la AC-CGCOM de cualquier inexactitud detectada en el certificado una vez se haya emitido, así como de los cambios que se produzcan en la información aportada y/o registrada para la emisión del certificado.

4.4. Obligaciones de custodia

El suscriptor se obliga a custodiar toda la información que genere en su actividad como entidad de registro.

5. Obligaciones de los firmantes y creadores de sellos

5.1. Obligaciones de custodia

El firmante o creador de sellos se obliga a custodiar el código de identificación personal, las claves privadas, cuando existan la tarjeta o cualquier otro soporte técnico entregado por la AC-CGCOM y, si fuese necesario, las especificaciones propiedad de la AC-CGCOM que le sean suministradas.
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, dichas circunstancias han de ser notificadas inmediatamente a la AC-CGCOM directamente o por medio del suscriptor.

5.2. Obligaciones de uso correcto

El firmante o creador de sellos tiene que utilizar el servicio de certificación prestado por la AC-CGCOM, exclusivamente para los usos autorizados en la DPC y en cualquier otra instrucción, manual o procedimiento suministrado al suscriptor.

El firmante o creador de sellos tiene que cumplir cualquier ley y regulación que pueda afectar a su derecho de uso de las herramientas criptográficas empleadas.

El firmante o creador de sellos no podrá adoptar medidas de inspección, alteración o descompilación de los servicios de certificación digital prestados.
El firmante o creador de sellos debe dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación, o de compromiso de las claves de la CA.

El firmante o creador de sellos reconocerá:

a) Que cuando utilice cualquier certificado, y mientras el certificado no haya expirado ni haya sido suspendido o haya sido revocado, habrá aceptado dicho certificado y estará operativo.
b) Que no actúa como entidad de certificación y, por lo tanto, se obliga a no utilizar las claves privadas correspondientes a las claves públicas contenidas en los certificados con el propósito de firmar certificado alguno.

5.3. Transacciones prohibidas

El firmante o creador de sellos se obliga a no utilizar sus claves privadas, los certificados, las tarjetas o cualquier otro soporte técnico entregado por la AC-CGCOM en la realización de transacción alguna prohibida por la ley aplicable.

Los servicios de certificación digital prestados por la AC-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 la operación de instalaciones nucleares, sistemas de navegación o comunicación aérea, sistemas de control de tráfico aéreo o sistemas de control de armamento, en las que un error pudiera directamente causar la muerte, daños físicos o daños medioambientales graves.

6. Obligaciones de los verificadores

6.1. Decisión informada

La AC-CGCOM informa al verificador 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 dicho certificado.

Adicionalmente, el verificador reconocerá que el uso del Registro y de las Listas de Revocación de Certificados (en lo sucesivo, "las LRCs" o "las CRLs) de

la AC-CGCOM, se rigen por la DPC de la AC-CGCOM y se comprometerá a cumplir los requisitos técnicos, operativos y de seguridad descritos en la mencionada DPC.

6.2. Requisitos de verificación de la firma electrónica

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

La 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:

- Es necesario utilizar el software apropiado para la verificación de una firma digital 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.

- 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 el uso de la cadena más adecuada para verificarla.

- Es necesario comprobar el estado de revocación de los certificados de la cadena con la información suministrada al Registro de CGCOM (con CRLs, por ejemplo) para determinar la validez de todos los certificados de la cadena de certificados, ya que únicamente puede considerarse correctamente verificada una firma electrónica si todos y cada uno de los certificados de la cadena son correctos y se encuentran vigentes.

- Es necesario asegurar que todos los certificados de la cadena autorizan el uso de la clave privada por el suscriptor del certificado y el firmante, ya que existe la posibilidad de que algunos 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.

- Es necesario verificar técnicamente la firma de todos los certificados de la cadena antes de confiar en el certificado utilizado por el firmante.

Para proceder a cifrar un mensaje o documento por una persona, **cuando se disponga de esta funcionalidad**, se ha de utilizar la clave pública propia del destinatario. Dicha clave pública se puede obtener a partir de su certificado. Por lo tanto, es necesario verificar este certificado antes de proceder al cifrado.

6.3. Confianza en un certificado no verificado

Cuando se disponga de esta funcionalidad, queda prohibido cifrar mensajes para 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.

6.4. Efecto de la verificación

En virtud de la correcta verificación de estos certificados, de conformidad con este texto divulgativo (PDS), el verificador puede confiar en la identificación y, en su caso, clave pública del firmante, dentro de las limitaciones de uso correspondientes, para generar mensajes cifrados.

6.5. 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 CGCOM, en la realización de transacción alguna prohibida para la ley aplicable a la citada transacción.

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

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

Los servicios de certificación digital prestados por CGCOM 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.

6.6. Cláusula de indemnidad

El tercero que confía en el certificado se compromete a mantener indemne a la CGCOM 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.

CGCOM no será responsable de los daños y perjuicios ocasionados, en los términos indicados en el artículo 11 de Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

7. Obligaciones de la AC-CGCOM

7.1. En relación con la prestación del servicio de certificación digital

La AC- CGCOM se obliga a:

a) Emitir, entregar, administrar, 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 la AC-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, con anterioridad a la fecha de expiración de los certificados, de la posibilidad de renovarlos o la posibilidad de 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.

7.2. En relación con las comprobaciones del registro

La AC-CGCOM se obliga a la emisión de certificados en base a los datos suministrados por el suscriptor, por lo cual podrá 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 firmantes.

Estas comprobaciones podrán incluir la justificación documental aportada por el firmante por medio del suscriptor, si la AC-CGCOM lo considera necesario,

y cualquier otro documento e información relevantes facilitados por el suscriptor y/o el firmante.

En el caso que la AC-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 la AC-CGCOM corrija los datos sin gestión previa de la incidencia correspondiente con el suscriptor, deberá notificar los datos finalmente certificados al suscriptor.

La AC-CGCOM se reserva el derecho a no emitir el certificado, cuando considere que la justificación documental resulte insuficiente para la correcta identificación y autenticación del suscriptor y/o del firmante.

8. Garantías limitadas y rechazo de garantías

8.1. Garantía de la AC-CGCOM por los servicios de certificación digital

La AC-CGCOM garantiza al suscritor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Entidad de Certificación.
- Que no hay errores de hecho en las informaciones contenidas en los certificados, debidos a falta de la diligencia debida en la gestión de la solicitud de certificado o en la creación de este.
- Que los certificados cumplen con todos los requisitos materiales establecidos en la DPC.
- Que los servicios de revocación y el empleo del depósito cumplen con todos los requisitos materiales establecidos en la DPC.

La AC-CGCOM garantiza al tercero que confía en el certificado:

- Que la información contenida o incorporada por referencia en el certificado es correcta, excepto cuando se indique lo contrario.

- En caso de certificados publicados en el depósito, que el certificado ha sido emitido al suscriptor y firmante identificado en el mismo y que el certificado ha sido aceptado.

- Que en la aprobación de la solicitud de certificado y en la emisión del certificado se han cumplido todos los requisitos materiales establecidos en la DPC.

- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y depósito.

Adicionalmente, la AC-CGCOM garantiza al suscriptor y al tercero que confía en el certificado:

- Que el certificado contiene las informaciones que debe contener un certificado cualificado, de acuerdo con el Anexo I del Reglamento UE 910/2014.

- Que, en el caso de que genere las claves privadas del firmante o, en su caso, persona física identificada en el certificado, se mantiene su confidencialidad durante el proceso.

- La responsabilidad de la Entidad de Certificación, con los límites que se establezcan. En ningún caso, la AC-CGCOM responderá por caso fortuito y en caso de fuerza mayor.
- La clave privada de la entidad de certificación utilizada para emitir certificados no ha sido comprometida, a menos que AC-CGCOM no haya comunicado lo contrario mediante el Registro de certificación, de acuerdo con la DPC.

- No ha originado ni ha introducido declaraciones falsas o erróneas en la información de ningún certificado, ni ha dejado de incluir información necesaria aportada por el suscriptor y validada por la AC-CGCOM, en el momento de la emisión del certificado.

- Todos los certificados cumplen los requisitos formales y de contenido de la DPC, incluyendo todos los requisitos legales en vigor y aplicables.

- Queda vinculada por los procedimientos operativos y de seguridad descritos en la DPC.

8.2. Exclusión de la garantía

La AC-CGCOM rechaza toda otra garantía diferente a la anterior que no sea legalmente exigible.

Específicamente, la AC-CGCOM no garantiza software alguno utilizado por cualquier persona para firmar, verificar firmas, cifrar, descifrar, o utilizar de otra forma certificado digital alguno emitido por la AC-CGCOM, excepto en los casos en que exista una declaración escrita en sentido contrario.

9. Acuerdos aplicables y DPC

9.1. Acuerdos aplicables

Los acuerdos aplicables a estos certificados son los siguientes:

- Convenio de colaboración de servicios de certificación, que regula la relación entre la AC-CGCOM y el Colegio, Servicio Autonómico de Salud o persona jurídica suscriptora de los certificados.

- Condiciones Generales del Servicio incorporadas en este texto de divulgación del certificado o PDS.

- DPC, que regula la emisión y utilización de los certificados.

9.2. Declaración de prácticas de certificación

Los servicios de certificación de la AC-CGCOM se regulan técnica y operativamente por la Declaración de prácticas de certificación de la AC-CGCOM por sus actualizaciones posteriores, así como por documentación complementaria.
La DPC y la documentación de operaciones se modifica periódicamente en el Registro y se puede consultar en la página de Internet: https://psc.cgcom.es

9.3. Política de certificación

La AC-CGCOM dispone de una política de certificación que detalla los requisitos de carácter técnico, jurídico, operativo, así como de regulación de los certificados, a disposición de la comunidad de usuarios que la soliciten.

10. Reglas de confianza para firmas longevas

La AC-CGCOM informa a los solicitantes de los certificados que no ofrece un servicio que garantice la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

La AC-CGCOM recomienda, para la fiabilidad de la firma electrónica de un documento a lo largo del tiempo, el uso de las reglas de confianza para firmas longevas recogidas en el apartado IV.3 de la NTI de Política de Firma y Sello Electrónicos y de Certificados de la Administración (Resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas)

11. Política de intimidad

La AC-CGCOM no puede divulgar ni puede ser obligada a divulgar información confidencial alguna en lo referente a certificados sin una solicitud específica previa que provenga de:

· la persona con respecto a la cual la AC-CGCOM tiene el deber de mantener la información confidencial, o

· una orden judicial, administrativa o cualquier otra prevista en la legislación vigente.

Sin embargo, el suscriptor acepta que determinada información, personal y de otro tipo, proporcionada en la solicitud de certificados, será incluida en sus certificados y en el mecanismo de comprobación del estado de los certificados, y que la información mencionada no tendrá carácter confidencial, por imperativo legal.

La AC-CGCOM no cede a ninguna persona los datos entregados específicamente para la prestación del servicio de certificación.

El tratamiento de dichos datos por motivo de la prestación del servicio de certificación de la AC-CGCOM por parte de Vintegris, entre otros, a título meramente enunciativo pero no limitativo, , se produce en el marco de un encargo del tratamiento(donde AC-CGCOM es responsable del tratamiento de los datos personales y Vintegris Encargado del Tratamiento de los mismos) a que se refiere el artículo 28 REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), y 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) y en su virtud es conforme con los requisitos del RGPD y de la LOPDGDD, y garantiza la protección de los derechos del interesado.

12. Política de privacidad

La AC-CGCOM dispone de una política de privacidad en el apartado 9.4 de la DPC, y regulación específica de la privacidad en relación con el proceso de registro, la confidencialidad del registro, la protección del acceso a la información personal, y el consentimiento del usuario.

Asimismo, AC-CGCOM conserva la información relativa a los servicios prestados de acuerdo con el artículo 24.2.h) del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, durante al menos 15 años desde la extinción del certificado o la finalización del servicio prestado.

13. Política de reintegro

La AC-CGCOM no reintegrará el coste del servicio de certificación en ningún caso.

14. Ley aplicable, jurisdicción competente y régimen de reclamaciones y disputas

Las relaciones con la AC-CGCOM se regirán por las leyes españolas en materia de servicios de confianza vigente en cada momento, así como por la legislación civil y mercantil en lo que sea de aplicación.

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

En caso de discrepancia entre las partes, las partes intentarán la previa resolución amistosa. A tal fin, las partes deberán dirigir una comunicación a la AC-CGCOM por cualquier medio que deje constancia a la dirección de contacto indicada en el punto 1 de esta PDS.

Si las partes no alcanzasen un acuerdo al respecto, cualquiera de ellas podrá someter el conflicto a la jurisdicción civil, con sujeción a los Tribunales del domicilio social de la AC-CGCOM.

15. Acreditaciones

La AC-CGCOM se encuentra incluida en la lista de prestadores de confianza (TSL) española:
https://sedediatid.mineco.gob.es/Prestadores/Paginas/Inicio.aspx

La AC-CGCOM dispone de la cualificación “eIDAS-compliant” para los siguientes servicios:

1. Servicio de expedición de certificados electrónicos cualificados de firma electrónica

a) Certificados Corporativos de Médico Colegiado
b) Certificados Corporativos de Persona Física Vinculada
c) Certificados Corporativos de Representante de Persona Jurídica

2. Servicio de expedición de certificados electrónicos cualificados de sello electrónico

d) Certificados de Sello electrónico de Persona Jurídica

16. Vinculación con la lista de prestadores

La AC-CGCOM es prestador cualificado de servicios de certificación por lo que forma parte de la Lista de Prestadores cualificados (TSL) que mantiene el supervisor nacional y que se puede obtener en la siguiente dirección:

https://sedeaplicaciones.minetur.gob.es/Prestadores/

La AC-CGCOM está incluida en la "Trust List" de la Unión Europea como Prestador cualificado de servicios electrónicos de confianza:

https://webgate.ec.europa.eu/tl-browser/#/tl/ES/19

17. Divisibilidad de las cláusulas, supervivencia, acuerdo íntegro y notificación

Las cláusulas del presente texto de divulgación (PDS) son independientes entre sí, motivo por el cual, si cualquier cláusula es considerada inválida o inaplicable, el resto de las cláusulas de las seguirán siendo aplicables, excepto acuerdo expreso en contrario de las partes.

Los requisitos contenidos en las secciones de "Obligaciones y responsabilidad", de "Auditoría de conformidad" y de "Confidencialidad" de la DPC de la AC-CGCOM continuarán vigentes tras la terminación del servicio.

Este texto contiene la voluntad completa y todos los acuerdos entre las partes.

Las partes se notifican hechos mutuamente mediante un procedimiento de envío a la dirección certificacion@cgcom.es