

Perfiles de Certificados de la Entidad de Certificación

Organización Médica Colegial de España



1. Información general

1.1 Control documental

| | |
|-----------------------|--|
| Proyecto: | Documentación de prácticas de la Entidad de Certificación |
| Entidad de destino: | Organización Médica Colegial de España |
| Código de referencia: | PT.01 |
| Versión: | 3.3 |
| Fecha de la edición: | 18/01/2012 |
| Archivo: | Perfiles_CGCOM_v3r3 |
| Formato: | Word 97-2003 |
| Autores: | Astrea |

1.2 Estado formal

| Preparado por: | Revisado por: | Aprobado por: |
|--|-----------------------|-----------------------|
| Nombre: Astrea Fecha: 18/01/2012 | Nombre: OMC Fecha: | Nombre: OMC Fecha: |

1.3 Control de versiones

| Versión | Partes que cambian | Descripción cambio | Autor cambio | Fecha cambio |
|----------------|---------------------------|---|---------------------|---------------------|
| 1.0 | Todo | Original | Astrea | 18/07/2006 |
| 2.0 | Perfiles | Revisión OMC | Astrea | 09/08/2006 |
| 2.1 | Perfiles | Revisión VeriSign | Astrea | 19/09/2006 |
| 2.2 | Perfiles | Corrección OIDs política | Astrea | 25/09/2006 |
| 3.0 | Perfiles | Adición perfiles externos | Astrea | 15/12/2009 |
| 3.1 | Perfil externos | Adición Pol. Certica | Astrea | 22/03/2011 |
| 3.2 | Perfil software y otras | . Adición Perfil Persona Jurídica en software . Mejoras en el campo Qualified Certificate Statements de todos los perfiles | Astrea | 13/07/2011 |
| 3.3 | Perfiles | . Alineación con el contenido de los diversos certificados emitidos. . Se amplía el Issuer Alternative Name | Astrea | 18/01/2012 |

1.4 Referencias

- Política de certificación VeriSign Trust Network.
- Política de certificación de la Organización Médica Colegial de España.
- 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. (B.O.E. 15-05-2003).
- Esquema de identificación y firma electrónica de las Administraciones públicas. Bloque I: Perfiles de certificados electrónicos (v1.7.3) CertiCA

2. Índice

| | |
|--|-----------|
| 1. Información general | 2 |
| 1.1 Control documental | 2 |
| 1.2 Estado formal | 2 |
| 1.3 Control de versiones | 3 |
| 1.4 Referencias | 3 |
| 2. Índice | 4 |
| 3. Introducción | 5 |
| 3.1 Tipología de certificados a expedir | 5 |
| 3.2 Perfiles efectivos a implantar | 7 |
| 4. Certificado corporativo de colegiado (persona física) | 8 |
| 5. Certificado corporativo de órgano colegial (persona física) | 13 |
| 6. Certificado corporativo de personal administrativo (persona física) | 18 |
| 7. Certificado corporativo de colegio profesional (persona jurídica) | 23 |
| 8. Certificado externo de colectivo de médico de servicio autonómico de salud (persona física) | 28 |
| 9. Certificado corporativo de colegio profesional (persona jurídica) en software | 33 |

3. Introducción

3.1 Tipología de certificados a expedir

La política de certificación de la Organización Médica Colegial determina la posibilidad de expedir los siguientes tipos de certificados:

a) Certificados de firma y certificados de cifrado

En cuanto al uso, existen dos tipos de certificados:

- 1) Certificados de firma electrónica, reconocidos, que se emplean como base de la firma electrónica avanzada, y en conjunción con un dispositivo seguro de creación de firma. También se pueden emplear para firmar mensajes de autenticación (confirmación de la identidad), así como para firmar otros tipos de mensajes.
- 2) Certificados de cifrado, ordinarios, que se emplean para producir o recibir documentos y mensajes cifrados.

b) Certificados corporativos y certificados externos

Los certificados de entidad final pueden ser certificados corporativos o certificados externos:

- 1) Los certificados corporativos se caracterizan por el hecho de que el suscriptor pertenece a una de las entidades que integran la Organización Médica Colegial. Los certificados corporativos siempre son de colectivo.
- 2) Los certificados externos son los restantes certificados. Es necesario realizar un registro completo de los datos a certificar.

Únicamente se expiden certificados externos, excepto cuando resulte necesario, como por ejemplo en el caso de médicos, colegiados o no, de un servicio autonómico de salud. Los certificados externos pueden ser individuales o de colectivo:

- a) Certificados externos individuales, caracterizados por el hecho de que la persona identificada en el certificado actúa en su propio nombre y representación (siendo en este caso el suscriptor o titular del certificado)
- b) Certificados externos de colectivo, en los que la persona identificada en el certificado actúa dentro del ámbito organizativo de una persona jurídica (que será el suscriptor o titular del certificado). Por ejemplo, los certificados emitidos a médicos, colegiados o no, adscritos a un servicio autonómico de salud serán certificados externos de colectivo, donde el suscriptor será el citado servicio autonómico de salud.

Los certificados externos de colectivo emitidos a un médico colegiado adscrito a un servicio autonómico de salud pueden incluirse en la tarjeta profesional que el Colegio expide al médico colegiado, en cuyo caso la tarjeta incluirá dos certificados.

Asimismo, el certificado externo de colectivo podrá ser expedido de forma remota con la autenticación basada en la firma electrónica reconocida del médico colegiado.

c) Certificados de colegiado y certificados de personal administrativo

Los certificados corporativos pueden expedirse a colegiados o a personal administrativo:

1) Certificados de colegiado, emitidos con la intervención de su Colegio de Médicos, en calidad de registrador con la capacidad exclusiva de certificar la cualidad de “colegiado” de una persona identificada en el certificado.

2) Certificados de personal administrativo de las entidades que integran la Organización Médica Colegial.

d) Certificados de persona física y certificados de persona jurídica

Los certificados pueden expedirse a personas físicas o a personas jurídicas:

1) Certificados de persona física, que actúa como firmante, debiendo tomarse en cuenta sus apoderamientos y capacidades de actuación, indicadas o no en el certificado, antes de confiar en la firma.

2) Certificados de persona jurídica, a la cual se imputan los documentos firmados, como firmante, sin que sea necesario tener en cuenta los apoderamientos o capacidades de actuación de la persona que custodia el certificado de firma electrónica.

3.2 Perfiles efectivos a implantar

Este documento recoge los perfiles de certificados que expedirá la Entidad de Certificación de la Organización Médica Colegial del España, con las siguientes consideraciones:

- Se ha considerado oportuno unificar los certificados de firma electrónica y cifrado, dado que en ningún caso se van a prestar servicios de recuperación de claves privadas de cifrado, debido a la sensibilidad de la información sanitaria.
- Se definen cinco perfiles de certificados corporativos: tres perfiles corresponden a certificados de persona física (colegiado, orgánico y de personal administrativo), uno al certificado de persona jurídica (colegio profesional) en tarjeta y uno al certificado de persona jurídica (colegio profesional) en software.
- Se define un único perfil de certificado externo de colectivo, para los médicos adscritos a un servicio autonómico de salud, colegiados o no colegiados.

Los certificados a expedir se basan en la política de clase 2 de la VeriSign Trust Network, que cabe indicar como segunda política de certificación, en los propios certificados.

Los certificados se expedirán en tarjeta criptográfica con la consideración de dispositivo seguro de creación de firma, y durarán un máximo de tres años, con re-autenticación anual de los poseedores de claves, mediante procedimientos organizativos, a excepción del certificado en software de persona jurídica.

El OID de OMC es 1.3.6.1.4.1.26852

4. Certificado corporativo de colegiado (persona física)

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|--|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ¹ | Sí | |
| 1.2. Serial Number | Establecido automáticamente ² | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ³ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ⁴ | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ⁵ | Sí | |

¹ El literal "2" corresponde a la versión 3.

² No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³ El texto se incluye sin acentos.

⁴ El texto se incluye sin acentos.

⁵ El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello deriva de

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|---|-------------|---------|
| 1.6.2. Organization (O) | Colegio profesional | Sí | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertCol(c)06 ” | Sí | |
| 1.6.4. Organizational Unit (OU) | “Use is subject to terms at https://www.verisign.com/rpa(c)99 ” | Sí | |
| 1.6.5. Surname | Apellidos | Sí | |
| 1.6.6. Given Name | Nombre | Sí | |
| 1.6.7. Title | “Médico colegiado/a” | Sí | |
| 1.6.8. Serial Number | DNI/NIE ⁶ | Sí | |
| 1.6.9. Common Name (CN) | “(Col.)” + Nombre y apellidos + “_” + Número de colegiado | Sí | |
| 1.6.10. Email (E) | Dirección de correo electrónico | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | Seleccionado. “1” | Sí | |

la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

⁶ El campo “número de serie” debe incluir el DNI o el NIE del colegiado, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.3.2. Non Repudiation | Seleccionado. "1" | Sí | |
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.4.3. QcSSCD (0.4.0.1862.1.4) | | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.1.1 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | "https://www.cgcom.es/CertCol" | Sí | |
| 2.5.2.2. User Notice | "Certificado corporativo de firma electrónica reconocida y cifrado de médico colegiado/a. Condiciones de uso en https://www.cgcom.es/CertCol " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|-----------------------------------|--|-------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del colegiado/a ⁷ | Sí | |
| 2.6.2. directoryName ⁸ | | Sí | |
| 2.6.2.1. CGCOM.2.1 | IdColegio | Sí | |
| 2.6.2.2. CGCOM.2.2 | Colegio profesional | Sí | |
| 2.6.2.3. CGCOM.2.3 | IdColegiado | Sí | |
| 2.6.2.4. CGCOM.2.4 | Nombre y apellidos del colegiado | Sí | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | "certificacion@cgcom.es" | Sí | |
| 2.7.2. directoryName | | Sí | |
| 2.7.2.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.7.2.2. SerialNumber | "Q2866017C" | Sí | |
| 2.7.2.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.7.2.4. Postal Code | "28014" | Sí | |
| 2.7.2.5. State Or Province Name | "Madrid" | Sí | |
| 2.7.2.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |
| 2.9. cRLDistributionPoint | | Sí | |

⁷ Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

⁸ Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.9.1. distributionPoint | "http://cr1.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.9.2. distributionPoint | "http://cr2.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |

5. Certificado corporativo de órgano colegial (persona física)

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|--|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ⁹ | Sí | |
| 1.2. Serial Number | Establecido automáticamente ¹⁰ | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ¹¹ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ¹² | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ¹³ | Sí | |

⁹ El literal "2" corresponde a la versión 3.

¹⁰ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹¹ El texto se incluye sin acentos.

¹² El texto se incluye sin acentos.

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|---|-------------|---------|
| 1.6.2. Organization (O) | Colegio profesional | Sí | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertOrg(c)06 ” | Sí | |
| 1.6.4. Organizational Unit (OU) | “Use is subject to terms at https://www.verisign.com/rpa(c)99 ” | Sí | |
| 1.6.5. Surname | Apellidos | Sí | |
| 1.6.6. Given Name | Nombre | Sí | |
| 1.6.7. Title | Órgano / cargo | Sí | |
| 1.6.8. Serial Number | DNI/NIE ¹⁴ | Sí | |
| 1.6.9. Common Name (CN) | Nombre y apellidos | Sí | |
| 1.6.10. Email (E) | Dirección de correo electrónico | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | Seleccionado. “1” | Sí | |

¹³ El campo “país” siempre será España, dado que el certificado muestra la relación entre una persona que ostenta un órgano o cargo y un colegio profesional español, con independencia de la nacionalidad de dicha persona.

¹⁴ El campo “número de serie” debe incluir el DNI o el NIE del órgano, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

| Campo | Contenido | Obligatorio | Crítico |
|---|--|-------------|---------|
| 2.3.2. Non Repudiation | Seleccionado. "1" | Sí | |
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.4.3. QcSSCD (0.4.0.1862.1.4) | | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.1.4 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | "https://www.cgcom.es/CerOrg" | Sí | |
| 2.5.2.2. User Notice | "Certificado corporativo de firma electrónica reconocida y cifrado de órgano colegial. Condiciones de uso en https://www.cgcom.es/CertOrg " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|------------------------------------|--|-------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del órgano ¹⁵ | Sí | |
| 2.6.2. directoryName ¹⁶ | | Sí | |
| 2.6.2.1. CGCOM.2.1 | IdColegio | Sí | |
| 2.6.2.2. CGCOM.2.2 | Colegio profesional | Sí | |
| 2.6.2.3. CGCOM.2.5 | IdOrgano | Sí | |
| 2.6.2.4. CGCOM.2.6 | Descripción del órgano colegial | Sí | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | "certificacion@cgcom.es" | Sí | |
| 2.11.3. directoryName | | Sí | |
| 2.11.3.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.11.3.2. SerialNumber | "Q2866017C" | Sí | |
| 2.11.3.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.11.3.4. Postal Code | "28014" | Sí | |
| 2.11.3.5. State Or Province Name | "Madrid" | Sí | |
| 2.11.3.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |
| 2.9. cRLDistributionPoint | | Sí | |

¹⁵ Este campo contiene la dirección de correo corporativo del órgano, a efectos de notificaciones.

¹⁶ Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.9.1. distributionPoint | "http://cr1.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.9.2. distributionPoint | "http://cr2.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |

6. Certificado corporativo de personal administrativo (persona física)

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|--|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ¹⁷ | Sí | |
| 1.2. Serial Number | Establecido automáticamente ¹⁸ | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ¹⁹ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ²⁰ | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ²¹ | Sí | |

¹⁷ El literal "2" corresponde a la versión 3.

¹⁸ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

¹⁹ El texto se incluye sin acentos.

²⁰ El texto se incluye sin acentos.

²¹ El campo "país" siempre será España, dado que el certificado muestra la relación entre un trabajador y un colegio profesional español, con independencia de la nacionalidad del trabajador.

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|---|-------------|---------|
| 1.6.2. Organization (O) | Colegio profesional | Sí | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertAdmin(c)06 ” | Sí | |
| 1.6.4. Organizational Unit (OU) | “Use is subject to terms at https://www.verisign.com/rpa(c)99 ” | Sí | |
| 1.6.5. Surname | Apellidos | Sí | |
| 1.6.6. Given Name | Nombre | Sí | |
| 1.6.7. Title | “Personal administrativo y de servicios” | Sí | |
| 1.6.8. Serial Number | DNI/NIE ²² | Sí | |
| 1.6.9. Common Name (CN) | Nombre y apellidos | Sí | |
| 1.6.10. Email (E) | Dirección de correo electrónico | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | Seleccionado. “1” | Sí | |
| 2.3.2. Non Repudiation | Seleccionado. “1” | Sí | |

²² El campo “número de serie” debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.4.3. QcSSCD (0.4.0.1862.1.4) | | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.1.2 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | https://www.cgcom.es/CertAdmin | Sí | |
| 2.5.2.2. User Notice | "Certificado corporativo de firma electrónica reconocida y cifrado de personal administrativo y de servicios. Condiciones de uso en https://www.cgcom.es/CertAdmin " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|------------------------------------|--|-------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del personal administrativo ²³ | Sí | |
| 2.6.2. directoryName ²⁴ | | Sí | |
| 2.6.2.1. CGCOM.2.1 | IdColegio | Sí | |
| 2.6.2.2. CGCOM.2.2 | Colegio profesional | Sí | |
| 2.6.2.3. CGCOM.2.7 | IdPersonalAdmin | Sí | |
| 2.6.2.4. CGCOM.2.8 | Nombre y apellidos del personal administrativo | Sí | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | "certificacion@cgcom.es" | Sí | |
| 2.7.2. directoryName | | Sí | |
| 2.7.2.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.7.2.2. SerialNumber | "Q2866017C" | Sí | |
| 2.7.2.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.7.2.4. Postal Code | "28014" | Sí | |
| 2.7.2.5. State Or Province Name | "Madrid" | Sí | |
| 2.7.2.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |

²³ Este campo contiene la dirección de correo corporativo del personal administrativo y de servicios, a efectos de notificaciones.

²⁴ Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.9. cRLDistributionPoint | | Sí | |
| 2.9.1. distributionPoint | "http://cr1.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.9.2. distributionPoint | "http://cr2.cgcom.es/cr/ec-cgcom.cr" | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |

7. Certificado corporativo de colegio profesional (persona jurídica)

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|---|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ²⁵ | Sí | |
| 1.2. Serial Number | Establecido automáticamente ²⁶ | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ²⁷ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ²⁸ | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ²⁹ | Sí | |

²⁵ El literal "2" corresponde a la versión 3.

²⁶ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

²⁷ El texto se incluye sin acentos.

²⁸ El texto se incluye sin acentos.

²⁹ El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado y un colegio profesional español, con independencia de la nacionalidad del colegiado. Ello

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|--|-------------|---------|
| 1.6.2. Organization (O) | Colegio profesional u otra persona jurídica | Sí | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertJur (c)06” | Sí | |
| 1.6.4. Organizational Unit (OU) | “Use is subject to terms at https://www.verisign.com/rpa (c)99” | Sí | |
| 1.6.5. Surname | Apellidos del custodio | Sí | |
| 1.6.6. Given Name | Nombre del custodio | Sí | |
| 1.6.7. 1.3.6.1.4.1.18838.1.1 | DNI/NIE ³⁰ | Sí | |
| 1.6.8. Serial Number | NIF de la entidad ³¹ | Sí | |
| 1.6.9. Common Name (CN) | Colegio profesional u otra persona jurídica | Sí | |
| 1.6.10. Email (E) | Dirección de correo electrónico | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |

deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y el colegiado, la persona autorizada a su uso.

³⁰ El campo “número de serie” debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

³¹ De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

| Campo | Contenido | Obligatorio | Crítico |
|---|--|-------------|---------|
| 2.3.1. Digital Signature | Seleccionado. "1" | Sí | |
| 2.3.2. Non Repudiation | Seleccionado. "1" | Sí | |
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.4.3. QcSSCD (0.4.0.1862.1.4) | | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.1.3 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | "https://www.cgcom.es/CertJur" | Sí | |
| 2.5.2.2. User Notice | "Certificado corporativo de firma electrónica reconocida y cifrado de persona jurídica. Condiciones de uso en https://www.cgcom.es/CertJur " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|------------------------------------|---|-------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del custodio ³² | Sí | |
| 2.6.2. directoryName ³³ | | Sí | |
| 2.6.2.1. CGCOM.2.1 | IdColegio | Sí | |
| 2.6.2.2. CGCOM.2.2 | Colegio profesional | Sí | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | "certificacion@cgcom.es" | Sí | |
| 2.7.2. directoryName | | Sí | |
| 2.7.2.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.7.2.2. SerialNumber | "Q2866017C" | Sí | |
| 2.7.2.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.7.2.4. Postal Code | "28014" | Sí | |
| 2.7.2.5. State Or Province Name | "Madrid" | Sí | |
| 2.7.2.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |
| 2.9. cRLDistributionPoint | | Sí | |
| 2.9.1. distributionPoint | "http://crl1.cgcom.es/crl/ec-cgcom.crl" | Sí | |

³² Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

³³ Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.9.2. distributionPoint | "http://crl2.cgcom.es/crl/ec-cgcom.crl" | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |

8. Certificado externo de colectivo de médico de servicio autonómico de salud (persona física)

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|---|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ³⁴ | Sí | |
| 1.2. Serial Number | Establecido automáticamente ³⁵ | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ³⁶ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ³⁷ | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ³⁸ | Sí | |

³⁴ El literal "2" corresponde a la versión 3.

³⁵ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

³⁶ El texto se incluye sin acentos.

³⁷ El texto se incluye sin acentos.

³⁸ El campo "país" siempre será España, dado que el certificado muestra la relación entre un empleado y un servicio autonómico de salud español, con independencia de la nacionalidad del

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|--|-------------|---------|
| 1.6.2. Organization (O) | Nombre del servicio autonómico de salud | Sí | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertECSAS(c)09 ” | Sí | |
| 1.6.4. Organizational Unit (OU) | Unidad administrativa | No | |
| 1.6.5. Organizational Unit (OU) | Número de empleado | No | |
| 1.6.6. Surname | Apellidos + “ – “ + NIF del empleado | Sí | |
| 1.6.7. Given Name | Nombre | Sí | |
| 1.6.8. Title | “Certificado electrónico de empleado público médico” | Sí | |
| 1.6.9. Serial Number | DNI/NIE del empleado público | Sí | |
| 1.6.10. Common Name (CN) | Nombre, apellidos + “ – “ + NIF del empleado | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | Seleccionado. “1” | Sí | |

empleado. Ello deriva de la naturaleza colectiva del certificado externo, del cual es suscriptor el servicio autonómico de salud, y el empleado, la persona autorizada a su uso.

| Campo | Contenido | Obligatorio | Crítico |
|---|--|-------------|---------|
| 2.3.2. Non Repudiation | Seleccionado. "1" | Sí | |
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.4.3. QcSSCD (0.4.0.1862.1.4) | | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.2.1 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | "https://www.cgcom.es/CertECSAS" | Sí | |
| 2.5.2.2. User Notice | "Certificado de firma electrónica reconocida y cifrado de médico del servicio autonómico de salud. Condiciones de uso en https://www.cgcom.es/CertECSAS " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|---|--|-----------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del empleado/a ³⁹ | Sí | |
| 2.6.2. Directory Name | | Sí | |
| 2.6.2.1. Tipo de certificado - OID 2.16.724.1.3.5.3.2.1 | Certificado electrónico de empleado público | F ⁴⁰ | |
| 2.6.2.2. Nombre de la entidad suscriptora - OID 2.16.724.1.3.5.3.2.2 | Nombre de la entidad suscriptora (servicio de salud) | F | |
| 2.6.2.3. NIF entidad suscriptora - OID 2.16.724.1.3.5.3.2.3 | NIF de la entidad suscriptora | F | |
| 2.6.2.4. DNI/NIE del responsable - OID 2.16.724.1.3.5.3.2.4 | DNI/NIE del responsable | F | |
| 2.6.2.5. Número de identificación de personal - OID 2.16.724.1.3.5.3.2.5 | Número de identificación del médico como empleado público | O ⁴¹ | |
| 2.6.2.6. Nombre de pila - OID 2.16.724.1.3.5.3.2.6 | Nombre de pila del médico – empleado público. | F | |
| 2.6.2.7. Primer apellido - OID 2.16.724.1.3.5.3.2.7 | Primer apellido del médico – empleado público | F | |
| 2.6.2.8. Segundo apellido - OID 2.16.724.1.3.5.3.2.8 | Segundo apellido del médico – empleado público | F | |
| 2.6.2.9. Correo electrónico - OID 2.16.724.1.3.5.3.2.9 | Correo electrónico del médico – empleado público | O | |
| 2.6.2.10. Unidad organizativa - OID 2.16.724.1.3.5.3.2.10 | Unidad, dentro de la Administración, en la que está incluida el médico – empleado público. | O | |

³⁹ Este campo contiene la dirección de correo corporativo del empleado, a efectos de notificaciones.

⁴⁰ Campo fijo (F), de acuerdo con perfiles Certica

⁴¹ Campo opcional (O), de acuerdo con perfiles Certica

| Campo | Contenido | Obligatorio | Crítico |
|--|---|-------------|---------|
| 2.6.2.11. Puesto o cargo - OID 2.16.724.1.3.5.3.2.1 1 | Puesto desempeñado por el médico – empleado público, dentro de la Administración | O | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | " certificacion@cgcom.es " | Sí | |
| 2.7.2. directoryName | | Sí | |
| 2.7.2.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.7.2.2. SerialNumber | "Q2866017C" | Sí | |
| 2.7.2.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.7.2.4. Postal Code | "28014" | Sí | |
| 2.7.2.5. State Or Province Name | "Madrid" | Sí | |
| 2.7.2.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |
| 2.9. cRLDistributionPoint | | Sí | |
| 2.9.1. distributionPoint | " http://cr1.cgcom.es/crl/ec-cgcom.crl " | Sí | |
| 2.9.2. distributionPoint | " http://cr2.cgcom.es/crl/ec-cgcom.crl " | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |

9. Certificado corporativo de colegio profesional (persona jurídica) en software

| Campo | Contenido | Obligatorio | Crítico |
|---------------------------------|---|-------------|---------|
| 1. Basic structure | | | |
| 1.1. Version | "2" ⁴² | Sí | |
| 1.2. Serial Number | Establecido automáticamente ⁴³ | Sí | |
| 1.3. Signature Algorithm | SHA-1 with RSA Signature | Sí | |
| 1.4. Issuer Distinguished Name | | Sí | |
| 1.4.1. Country (C) | "ES" | Sí | |
| 1.4.2. Organization (O) | "Organizacion Medica Colegial" ⁴⁴ | Sí | |
| 1.4.3. Organizational Unit (OU) | "Entidad de Certificacion" ⁴⁵ | Sí | |
| 1.4.4. Organizational Unit (OU) | "Class 2 Managed PKI Individual Subscriber CA" | Sí | |
| 1.4.5. Organizational Unit (OU) | "VeriSign Trust Network" | Sí | |
| 1.4.6. Common Name (CN) | "OMC" | Sí | |
| 1.5. Validity | 3 años | Sí | |
| 1.5.1. Not Before | Fecha de inicio de validez | Sí | |
| 1.5.2. Not After | Fecha de expiración | Sí | |
| 1.6. Subject | | Sí | |
| 1.6.1. Country (C) | "ES" ⁴⁶ | Sí | |
| 1.6.2. Organization (O) | Colegio profesional u otra | Sí | |

⁴² El literal "2" corresponde a la versión 3.

⁴³ No debe superar los 32 caracteres hexadecimales en notación hexadecimal.

⁴⁴ El texto se incluye sin acentos.

⁴⁵ El texto se incluye sin acentos.

⁴⁶ El campo "país" siempre será España.

| Campo | Contenido | Obligatorio | Crítico |
|----------------------------------|---|-------------|---------|
| | persona jurídica | | |
| 1.6.3. Organizational Unit (OU) | “Condiciones de uso en https://www.cgcom.es/CertJurSoft (c)11” | Sí | |
| 1.6.4. Organizational Unit (OU) | “Use is subject to terms at https://www.verisign.com/rpa (c)99” | Sí | |
| 1.6.5. Surname | Apellidos del custodio | Sí | |
| 1.6.6. Given Name | Nombre del custodio | Sí | |
| 1.6.7. 1.3.6.1.4.1.18838.1.1 | DNI/NIE ⁴⁷ | Sí | |
| 1.6.8. Serial Number | NIF de la entidad ⁴⁸ | Sí | |
| 1.6.9. Common Name (CN) | Colegio profesional u otra persona jurídica | Sí | |
| 1.6.10. Email (E) | Dirección de correo electrónico | Sí | |
| 1.7. Subject Public Key Info | 2048-Bit Public key encoded in accordance with RFC2459 & PKCS#1 | Sí | |
| 2. Extensions | | | |
| 2.1. Authority Key Identifier | Presente | Sí | |
| 2.1.1. Key Identifier | | | |
| 2.1.2. AuthorityCertIssuer | | | |
| 2.1.3. AuthorityCertSerialNumber | | | |
| 2.2. Subject Key Identifier | Presente | Sí | |
| 2.3. Key Usage | | Sí | Sí |
| 2.3.1. Digital Signature | Seleccionado. “1” | Sí | |
| 2.3.2. Non Repudiation | Seleccionado. “1” | Sí | |

⁴⁷ El campo “número de serie” debe incluir el DNI o el NIE del trabajador, al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

⁴⁸ De acuerdo con la normativa tributaria, en este campo debe figurar el NIF de la persona jurídica.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.3.3. Key Encipherment | Seleccionado. "1" | Sí | |
| 2.3.4. Data Encipherment | Seleccionado. "1" | Sí | |
| 2.3.5. Key Agreement | No seleccionado. "0" | | |
| 2.3.6. Key Certificate Signature | No seleccionado. "0" | | |
| 2.3.7. CRL Signature | No seleccionado. "0" | | |
| 2.4. Qualified Certificate Statements | | Sí | |
| 2.4.1. qCCompliance (0.4.0.1862.1.1) | | Sí | |
| 2.4.2. QcEuRetentionPeriod (0.4.0.1862.1.3) | 15 | Sí | |
| 2.5. Certificate Policies | | Sí | |
| 2.5.1. Policy Identifier | OMC.1.1.5 | Sí | |
| 2.5.2. Policy Qualifier ID | | Sí | |
| 2.5.2.1. CPS Pointer | "https://www.cgcom.es/CertJurSoft" | Sí | |
| 2.5.2.2. User Notice | "Certificado corporativo de firma electrónica avanzada y cifrado de persona jurídica en software. Condiciones de uso en https://www.cgcom.es/CertJurSoft " | Sí | |
| 2.5.3. Policy Identifier | OID de política de clase 2 de VeriSign | Sí | |
| 2.5.4. Policy Qualifier ID | | Sí | |
| 2.5.4.1. CPS Pointer | Referencia al VeriSign RPA | Sí | |
| 2.5.4.2. User Notice | Aviso de usuario de VeriSign | Sí | |

| Campo | Contenido | Obligatorio | Crítico |
|------------------------------------|---|-------------|---------|
| 2.6. Subject Alternative Names | | Sí | |
| 2.6.1. rfc822Name | Correo electrónico corporativo del custodio ⁴⁹ | Sí | |
| 2.6.2. directoryName ⁵⁰ | | Sí | |
| 2.6.2.1. CGCOM.2.1 | IdColegio | Sí | |
| 2.6.2.2. CGCOM.2.2 | Colegio profesional | Sí | |
| 2.7. Issuer Alternative Name | | Sí | |
| 2.7.1. rfc822Name | "certificacion@cgcom.es" | Sí | |
| 2.7.2. directoryName | | Sí | |
| 2.7.2.1. Organization (O) | "Consejo General de Colegios de Medicos" | Sí | |
| 2.7.2.2. SerialNumber | "Q2866017C" | Sí | |
| 2.7.2.3. Locality (L) | "Plaza de las Cortes 11" | Sí | |
| 2.7.2.4. Postal Code | "28014" | Sí | |
| 2.7.2.5. State Or Province Name | "Madrid" | Sí | |
| 2.7.2.6. Country (C) | ES | Sí | |
| 2.8. Extended Key Usage | | Sí | |
| 2.8.1. emailProtection | Presente | Sí | |
| 2.8.2. clientAuth | Presente | Sí | |
| 2.9. cRLDistributionPoint | | Sí | |
| 2.9.1. distributionPoint | "http://crl1.cgcom.es/crl/ec-cgcom.crl" | Sí | |

⁴⁹ Este campo contiene la dirección de correo corporativo del colegiado, a efectos de notificaciones.

⁵⁰ Este campo enlaza con el sistema de validación y re-certificación del CGCOM, permitiendo recuperar informaciones adicionales de forma eficiente. Ciertas informaciones se incluyen, aunque sean redundantes, para disponer de toda la información sobre el usuario en una sola consulta contra el certificado.

| Campo | Contenido | Obligatorio | Crítico |
|---|---|-------------|---------|
| 2.9.2. distributionPoint | "http://crl2.cgcom.es/crl/ec-cgcom.crl" | Sí | |
| 2.10. NetscapeCertType | "SSL client", "S/MIME" | Sí | |
| 2.11. Subject Directory Attributes (2.5.29.9) | | Sí | |
| 2.11.1. Country of Citizenship | País de nacionalidad | Sí | |
| 2.11.2. Country of Residence | País de residencia | Sí | |