Servicio de Certificación Digital

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

Consejo General
de Colegios Oficiales de Médicos

Declaración de Prácticas de Certificación
Autoridad de Certificación del
Consejo General de Colegios Oficiales de Médicos

044

Control de versiones

Versión	Partes que cambian	Descripción del cambio	Autor del cambio	Fecha del cambio
4.0	Original	Creación documento	VINTEGRIS	18/11/2019
4.1.	1.5.3	Periodicidad revisión de sistemas	CGCOM	1/4/2020
4.2	4.9.13, 4.9.14, 4.9.15, 5.2.4, 5.3.8	Correcciones menores	ASTREA	08/04/2020
4.3	1.3.4.1, 6.5.3, 1.5.3.1, 1.5.3.2	Correcciones menores. Cambio proveedor QSCD. Procedimiento de revisión y aprobación del documento.	CGCOM	24/06/2020
4.4	1.3.4.2.1 1.4.1.2 1.4.1.3.3	Corrección OIDs. Actualización información autoridad de certificación subordinada	CGCOM	28/07/2019
4.5		Adaptación a ley 6/2020	ASTREA	07/05/2021
	1.2.1.2 1.4.1.7	Se añade apartado para certificados no cualificados	ASTREA	27/05/2021
4.6	3.2.3, 5.4, 5.8, 7.1, 7.2, 7.3	Correcciones menores tras auditoría de seguimiento	ASTREA	21/07/2021
4.7	6.1.6	Indicación de longitudes de los campos del *subject* de acuerdo con las normas ETSI.	ASTREA	22/04/2022
	3.1.1	Revisión	ASTREA	22/04/2022
	5.4.8	Plazo máximo resolución vulnerabilidades críticas	ASTREA	25/04/2022
	4.5.4	Revisión	ASTREA	30/05/2022
4.8		Revisión	ASTREA	13/03/2023
	1.3.4.2, 4.9.6, 4.9.9	Inclusión nueva CA	ASTREA	25/05/2023

Tabla de contenido

1 Introducción 12

1.1 Presentación 13

1.2 Nombre del documento e identificación 13

1.2.1 Identificadores de certificados actuales 13

1.3 Participantes en los servicios de certificación 15

1.3.1 Prestador de Servicios de Certificación 16

1.3.2 Registradores 16

1.3.3 Entidades finales 17

1.3.4 Otros participantes 19

1.4 Uso de los certificados 21

1.4.1 Usos permitidos para los certificados 21

1.4.2 Límites y prohibiciones de uso de los certificados 45

1.5 Administración de la política 46

1.5.1 Organización que administra el documento 46

1.5.2 Datos de contacto de la organización 47

1.5.3 Procedimientos de gestión del documento 47

1.6 Definiciones y acrónimos 48

1.6.1 Definiciones 48

1.6.2 Acrónimos 51

2 Publicación de información y depósito de certificados 55

2.1 Depósito(s) de certificados 55

2.2 Publicación de información del prestador de servicios de certificación 55

2.3 Frecuencia de publicación 55

2.4 Control de acceso 56

3 Identificación y autenticación 57

3.1 Registro inicial 57

3.1.1 Tipos de nombres 57

3.1.2 Significado de los nombres 59
3.1.3 Empleo de anónimos y seudónimos 59
3.1.4 Interpretación de formatos de nombres 59
3.1.5 Unicidad de los nombres 59
3.1.6 Resolución de conflictos relativos a nombres 60

3.2 Validación inicial de la identidad 61
3.2.1 Prueba de posesión de clave privada 61
3.2.2 Autenticación de la identidad de una organización 62
3.2.3 Autenticación de la identidad de una persona física 68
3.2.4 Información de suscriptor no verificada 69

3.3 Identificación y autenticación de solicitudes de renovación 69
3.3.1 Validación para la renovación rutinaria de certificados 69
3.3.2 Validación para la renovación de certificados tras la revocación 70

3.4 Identificación y autenticación de la solicitud de revocación 70

4 Requisitos de operación del ciclo de vida de los certificados 72

4.1 Solicitud de emisión de certificado 72
4.1.1 Legitimación para solicitar la emisión 72
4.1.2 Procedimiento de alta; Responsabilidades 72

4.2 Procesamiento de la solicitud de certificación 73
4.2.1 Ejecución de las funciones de identificación y autenticación 73
4.2.2 Aprobación o rechazo de la solicitud 73
4.2.3 Plazo para resolver la solicitud 74

4.3 Emisión del certificado 74
4.3.1 Acciones de la Autoridad de Certificación del CGCOM durante el proceso de emisión 74
4.3.2 Notificación de la emisión al suscriptor 75

4.4 Entrega y aceptación del certificado 75
4.4.1 Responsabilidades de la Autoridad de Certificación del CGCOM 76
4.4.2 Conducta que constituye aceptación del certificado 77
4.4.3 Publicación del certificado 77
4.4.4 Notificación de la emisión a terceros 77

4.5 Uso del par de claves y del certificado 77
4.5.1 Uso por el firmante 78
4.5.2 Responsabilidad civil del firmante 78

4.5.3 Uso por el suscriptor 79
4.5.4 Uso por el tercero que confía en certificados 80

4.6 Renovación de certificados 81
4.7 Renovación de claves y certificados 82
4.7.1 Causas de renovación de claves y certificados 82
4.7.2 Legitimación para solicitar la renovación 82
4.7.3 Procedimientos de solicitud de renovación 82
4.7.4 Notificación de la emisión del certificado renovado 83
4.7.5 Conducta que constituye aceptación del certificado 84
4.7.6 Publicación del certificado 84
4.7.7 Notificación de la emisión a terceros 84

4.8 Modificación de certificados 84
4.9 Revocación de certificados 84
4.9.1 Causas de revocación de certificados 84
4.9.2 Legitimación para solicitar la revocación 86
4.9.3 Procedimientos de solicitud de revocación 86
4.9.4 Plazo temporal de solicitud de revocación 88
4.9.5 Plazo temporal de procesamiento de la solicitud 88
4.9.6 Obligación de consulta de información de revocación de certificados 88
4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs) 89
4.9.8 Plazo máximo de publicación de LRCs 89
4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados 89
4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados 91
4.9.11 Otras formas de información de revocación de certificados 91
4.9.12 Requisitos especiales en caso de compromiso de la clave privada 91
4.9.13 Solicitud de suspensión 91
4.9.14 Procedimientos para la petición de suspensión 92
4.9.15 Período máximo de suspensión 92

4.10 Servicios de comprobación de estado de certificados 92
4.10.1 Características operativas de los servicios 92
4.10.2 Disponibilidad de los servicios 92
4.10.3 Características opcionales 92

4.11 Finalización de la suscripción 92
4.12 Depósito y recuperación de claves 93
4.12.1 Política y prácticas de depósito y recuperación de claves 93

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión 93

5 Controles de seguridad física, de gestión y de operaciones 94

5.1 Controles de seguridad física 94

5.1.1 Localización y construcción de las instalaciones 96
5.1.2 Acceso físico 96
5.1.3 Electricidad y aire acondicionado 97
5.1.4 Exposición al agua 97
5.1.5 Prevención y protección de incendios 98
5.1.6 Almacenamiento de soportes 98
5.1.7 Tratamiento de residuos 98
5.1.8 Copia de respaldo fuera de las instalaciones 99

5.2 Controles de procedimientos 99

5.2.1 Funciones fiables 100
5.2.2 Número de personas por tarea 101
5.2.3 Identificación y autenticación para cada función 101
5.2.4 Roles que requieren separación de tareas 101
5.2.5 Arranque y parada del sistema de gestión PKI 102

5.3 Controles de personal 102

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización 102
5.3.2 Procedimientos de investigación de historial 103
5.3.3 Requisitos de formación 104
5.3.4 Requisitos y frecuencia de actualización formativa 105
5.3.5 Secuencia y frecuencia de rotación laboral 105
5.3.6 Sanciones para acciones no autorizadas 105
5.3.7 Requisitos de contratación de profesionales 106
5.3.8 Suministro de documentación al personal 106

5.4 Procedimientos de auditoria de seguridad 106

5.4.1 Tipos de eventos registrados y su frecuencia 107
5.4.2 Frecuencia de tratamiento de registros de auditoría 109
5.4.3 Periodo de conservación de registros de auditoría 109
5.4.4 Protección de los registros de auditoría 109
5.4.5 Procedimientos de copia de respaldo 110
5.4.6 Localización del sistema de acumulación de registros de auditoría 110
5.4.7 Notificación del evento de auditoria al causante del evento 110
5.4.8 Análisis de vulnerabilidades 110

5.5 Archivo de informaciones ____ 111
5.5.1 Tipos de registros archivados ____ 111
5.5.2 Periodo de conservación de registros ____ 112
5.5.3 Protección del archivo ____ 113
5.5.4 Procedimientos de copia de respaldo ____ 113
5.5.5 Requisitos de sellado de fecha y hora ____ 114
5.5.6 Localización del sistema de archivo ____ 114
5.5.7 Procedimientos de obtención y verificación de información de archivo ____ 114
5.6 Renovación de claves ____ 115
5.7 Compromiso de claves y recuperación de desastre ____ 115
5.7.1 Procedimientos de gestión de incidencias y compromisos ____ 115
5.7.2 Corrupción de recursos, aplicaciones o datos ____ 116
5.7.3 Compromiso de la clave privada de la entidad ____ 117
5.7.4 Continuidad del negocio después de un desastre ____ 117
5.8 Terminación del servicio ____ 118
6 Controles de seguridad técnica ____ 121
6.1 Generación e instalación del par de claves ____ 121
6.1.1 Generación del par de claves ____ 121
6.1.2 Envío de la clave privada al suscriptor ____ 123
6.1.3 Envío de la clave pública al emisor del certificado ____ 123
6.1.4 Distribución de la clave pública del prestador de servicios de certificación ____ 123
6.1.5 Tamaños de claves ____ 124
6.1.6 Generación de parámetros de clave pública ____ 124
6.1.7 Comprobación de calidad de parámetros de clave pública ____ 124
6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo ____ 125
6.1.9 Propósitos de uso de claves ____ 125
6.2 Protección de la clave privada y controles de los módulos criptográficos ____ 125
6.2.1 Estándares de módulos criptográficos ____ 125
6.2.2 Control por más de una persona (n de m) sobre la clave privada ____ 127
6.2.3 Depósito de la clave privada ____ 127
6.2.4 Copia de respaldo de la clave privada ____ 127
6.2.5 Archivo de la clave privada ____ 127
6.2.6 Introducción de la clave privada en el módulo criptográfico ____ 128
6.2.7 Almacenamiento de la clave privada en el módulo criptográfico ____ 128
6.2.8 Método de activación de la clave privada ____ 128

6.2.9 Método de desactivación de la clave privada 128
6.2.10 Método de destrucción de la clave privada 129
6.2.11 Clasificación de módulos criptográficos 129

6.3 Otros aspectos de gestión del par de claves 129
6.3.1 Archivo de la clave pública 129
6.3.2 Periodos de utilización de las claves pública y privada 129

6.4 Datos de activación 129
6.4.1 Generación e instalación de datos de activación 130
6.4.2 Protección de datos de activación 130
6.4.3 Otros aspectos de los datos de activación 130

6.5 Controles de seguridad informática 130
6.5.1 Requisitos técnicos específicos de seguridad informática 131
6.5.2 Evaluación del nivel de seguridad informática 132
6.5.3 Periodicidad revisión de componentes del sistema mantenidos por CGCOM 132

6.6 Controles técnicos del ciclo de vida 132
6.6.1 Controles de desarrollo de sistemas 132
6.6.2 Controles de gestión de seguridad 132
6.6.3 AC-CGCOM Evaluación del nivel de seguridad del ciclo de vida 135

6.7 Controles de seguridad de red 135
6.8 Fuentes de Tiempo 136

7 Perfiles de certificados y listas de certificados revocados 137

7.1 Perfil de certificado 137
7.1.1 Número de versión 137
7.1.2 Extensiones del certificado 137
7.1.3 Identificadores de objeto (OID) de los algoritmos 137
7.1.4 Formato de Nombres 137
7.1.5 Restricciones de los nombres 138
7.1.6 Identificador de objeto (OID) de la Política de Certificación 138
7.1.7 Extensión del uso de las restricciones de política 138
7.1.8 Sintaxis y semántica de los “PolicyQualifier” 138
7.1.9 Tratamiento semántico para la extensión “Certificate Policy” 138

7.2 Perfil de la lista de revocación de certificados 139
7.2.1 Número de versión 139
7.2.2 CRL y extensiones 139

7.3 Perfil de OCSP 139
7.3.1 Número de versión 140
7.3.2 Extensiones del OCSP 140

8 Auditoria de conformidad ***141***

8.1 Frecuencia de la auditoria de conformidad 141
8.2 Identificación y calificación del auditor 142
8.3 Relación del auditor con la entidad auditada 142
8.4 Listado de elementos objeto de auditoria 142
8.5 Acciones a emprender como resultado de una falta de conformidad 143
8.6 Tratamiento de los informes de auditoría 143

9 Requisitos comerciales y legales ***144***

9.1 Tarifas 144
9.1.1 Tarifa de emisión o renovación de certificados 144
9.1.2 Tarifa de acceso a certificados 144
9.1.3 Tarifa de acceso a información de estado de certificado 144
9.1.4 Tarifas de otros servicios 144
9.1.5 Política de reintegro 144

9.2 Responsabilidad financiera 144
9.2.1 Cobertura de seguro 145
9.2.2 Otros activos 145
9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados 145

9.3 Confidencialidad de la información 145
9.3.1 Informaciones confidenciales 145
9.3.2 Informaciones no confidenciales 146
9.3.3 Divulgación de información de suspensión y revocación 146
9.3.4 Divulgación legal de información 147
9.3.5 Divulgación de información por petición de su titular 147
9.3.6 Otras circunstancias de divulgación de información 147

9.4 Protección de la información personal 147
9.5 Derechos de propiedad intelectual 148
9.5.1 Propiedad de los certificados e información de revocación 148
9.5.2 Propiedad de la Declaración de Prácticas de Certificación 149
9.5.3 Propiedad de la información relativa a nombres 149

9.5.4 Propiedad de claves 149

9.6 Obligaciones y responsabilidad civil 149

9.6.1 Obligaciones de la Autoridad de Certificación del CGCOM 149

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados 151

9.7 Exención de garantía 152

9.8 Responsabilidades 152

9.8.1 Responsabilidades de la Autoridad de Certificación 153

9.8.2 Responsabilidades de la Autoridad de Registro 153

9.8.3 Responsabilidades del suscriptor 154

9.8.4 Delimitación de responsabilidades 154

9.8.5 Cláusula de indemnidad de suscriptor 155

9.8.6 Cláusula de indemnidad de tercero que confía en el certificado 156

9.8.7 Caso fortuito y fuerza mayor 156

9.9 Indemnizaciones 156

9.9.1 Alcance de la cobertura 156

9.9.2 Limitaciones de pérdidas 157

9.10 Período de validez 157

9.10.1 Plazo 157

9.10.2 Sustitución y derogación de la DPC 157

9.10.3 Efectos de la finalización 157

9.11 Notificaciones individuales y comunicaciones con los participantes 157

9.12 Cambios en las especificaciones 158

9.12.1 Procedimiento para los cambios 158

9.12.2 Período y procedimiento de notificación 159

9.12.3 Circunstancias en las que el OID debe ser cambiado 159

9.13 Reclamaciones y resolución de conflictos 159

9.14 Normativa aplicable 159

9.15 Cumplimiento de la normativa aplicable 160

9.16 Otras disposiciones 160

9.16.1 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación 160

9.17 Otras provisiones 161

1 Introducción

El Consejo General de Colegios Oficiales de Médicos establece establece un sistema de certificación con los siguientes objetivos:

1) La emisión y gestión, por uno o más prestadores de servicios de certificación, de certificados cualificados de firma electrónica de médico colegiado y otro personal colegial, así como de otros servicios de certificación.
2) La acreditación, por el Consejo General de Colegios Oficiales de Médicos, de los diferentes prestadores de servicios de certificación que suministren certificados a los profesionales colegiados, al objeto de garantizar la calidad y seguridad en la emisión y gestión de los citados certificados.
3) La prestación de servicios de validación y re-certificación a entidades, públicas y privadas, sobre los certificados, al objeto de garantizar la actualidad y validez de las informaciones corporativas, incluidas o no en los certificados, y en especial, de la condición de médico.
4) La regulación de la emisión y gestión de los dispositivos cualificados de creación de firma electrónica a usar por el CGCOM.

En concreto, se definen los requisitos comunes tanto para la expedición de certificados por la Autoridad de Certificación Consejo General de Colegios Oficiales de Médicos, o por cualquier otro prestador de servicios de certificación corporativos, que debe ser acreditado por el Consejo General de Colegios Oficiales de Médicos, como para la validación y, en su caso, re-certificación de la condición corporativa de médico y otras informaciones, para certificados expedidos por cualesquiera prestadores de servicios de certificación, en las diferentes aplicaciones en que resulte necesario.

Todo ello se realiza sobre la base del certificado cualificado como instrumento de identificación y firma del médico colegiado, así como, en su caso, de otro personal colegial, frente a otros profesionales colegiales, las entidades y corporaciones públicas y privadas, y las Administraciones Públicas.

1.1 Presentación

Este documento declara las prácticas de certificación de firma electrónica de la Autoridad de Certificación del Consejo General de Colegios Oficiales de Médicos.

Los certificados que se emiten son los siguientes:

- Certificados **corporativos** de:
  - **Médico/a colegiado/a**
  - **Personas físicas vinculadas**
  - **Sello electrónico de persona jurídica**
  - **Representante legal de persona jurídica**

Los servicios de certificación prestados por la Autoridad de Certificación del CGCOM se encuentran integrados en la jerarquía de la Autoridad de Certificación de la empresa VÍNTEGRIS, que actúa en esta DPC como proveedor técnico.

La integración de la Autoridad de Certificación del CGCOM dentro de la jerarquía del proveedor técnico se ha realizado mediante la firma del certificado de la Autoridad de Certificación del CGCOM.

1.2 Nombre del documento e identificación

Este documento es la "Declaración de Prácticas de Certificación del Consejo General de Colegios Oficiales de Médicos".

1.2.1 Identificadores de certificados actuales

El Consejo General de Colegios Oficiales de Médicos ha asignado a cada política de certificado un identificador de objeto (OID), para su identificación por las aplicaciones.

1.2.1.1 Certificados cualificados

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

En caso de contradicción entre esta Declaración de Prácticas de Certificación y otros documentos de prácticas y procedimientos, prevalecerá lo establecido en esta Declaración de Prácticas de Certificación.

1.2.1.2 Certificados no cualificados

Tipo	Soporte	Usos	OID
De Sello electrónico de persona jurídica	En software	Autenticación, Firma y cifrado	• 1.3.6.1.4.1.26852.1.100.10.1 • 0.4.0.2042.1.2

1.3 Participantes en los servicios de certificación

Los servicios descritos en esta declaración de prácticas son prestados a una comunidad profesional de usuarios, que obtienen certificados para diversos usos y aplicaciones profesionales relacionadas con las entidades que integran el Consejo General de Colegios Oficiales de Médicos y aquellas otras entidades del ámbito sanitario con las que la CGCOM disponga un convenio de colaboración.

CGCOM no expide los certificados corporativos al público, ni siquiera cuando se trata de certificados cualificados, como el certificado de firma de colegiado.

1.3.1 Prestador de Servicios de Certificación

Los prestadores de servicios de certificación son personas, físicas o jurídicas, que expiden y gestionan certificados para entidades finales.

El papel del Consejo General de Colegios Oficiales de Médicos es doble:

- Por una parte, CGCOM garantiza la calidad en el empleo de los medios electrónicos, informáticos y telemáticos por los profesionales médicos, mediante la acreditación de los prestadores de servicios de certificación, de acuerdo con la política de certificación.
- Por otra parte, CGCOM dispone de una Autoridad de Certificación para la emisión y gestión de claves y certificados de entidad final, incluyendo personas, dentro del ámbito corporativo, a los propios colegios y otras personas jurídicas del ámbito sanitario.

1.3.2 Registradores

En general, los registradores de certificados corporativos son las entidades del Consejo General de Colegios Oficiales de Médicos, y en especial, los Colegios de Médicos.

Por su parte, el Consejo General de Colegios Oficiales de Médicos asiste técnicamente en el registro a los Colegios de Médicos.

1.3.3 Entidades finales

Las entidades finales son las personas y organizaciones destinatarias de los servicios de emisión, gestión y uso de certificados digitales, para los usos de firma electrónica, autenticación y cifrado.

Serán entidades finales del sistema de certificación del Consejo General de Colegios Oficiales de Médicos las siguientes entidades:

1) Solicitantes de certificados.
2) Suscriptores del servicio de certificación.
3) Firmantes y personas responsables de los datos de creación de sellos electrónicos .
4) Partes usuarias.

1.3.3.1 Solicitantes de certificados

Todo certificado debe ser solicitado por una persona, en su propio nombre o en nombre de una organización.

Pueden ser solicitantes:

1) El colegio que va a ser el futuro suscriptor del certificado. Dicho colegio puede establecer un modelo de solicitud de certificado por parte de los colegiados.
2) Una persona autorizada por dicho futuro suscriptor.
3) Otras personas jurídicas del ámbito sanitario que dispongan de convenio con CGCOM.

1.3.3.2 Suscriptores del servicio de certificación

Los suscriptores del servicio de certificación son las entidades que los adquieren a la Autoridad de Certificación para su uso en su ámbito corporativo, incluyendo los colegios profesionales y otras personas jurídicas del ámbito sanitario.

El suscriptor del servicio de certificación adquiere una licencia de uso del certificado, al objeto de facilitar el acceso al certificado a una persona concreta, debidamente autorizada, y que figura identificada en el certificado, como se indica en el siguiente epígrafe.

El suscriptor del servicio de certificación es, por tanto, el cliente de la Autoridad de Certificación, de acuerdo con la legislación mercantil, y tiene los derechos y obligaciones que se definen por la Autoridad de Certificación, que son adicionales y se entienden sin perjuicio de los derechos y obligaciones de los firmantes y las personas responsables de los datos de creación de los sellos electrónicos de persona jurídica, como se autoriza y regula en las normas técnicas europeas aplicables a la expedición de certificados electrónicos cualificados, en especial ETSI EN 319 411-2, secciones 5.4.2 y 6.3.4.e)

1.3.3.3 Firmantes y creadores de sellos

Los firmantes son las personas físicas que poseen de forma exclusiva las claves de firma digital (para identificación y firma electrónica) y de descifrado del certificado; esto es, típicamente los colegiados/as, las personas física vinculadas (como los órganos colegiales y el personal administrativo), y los representantes legales.,

Los creadores de sellos son aquellas personas responsables de los datos de creación de los sellos electrónicos de persona jurídica.

Los firmantes y personas responsables de los datos de creación de sellos electrónicos de persona jurídica se encuentran debidamente autorizados por el suscriptor.

La clave privada de descifrado no puede ser recuperada, actualmente, por el prestador de servicios de certificación, por lo que las personas físicas identificadas en los correspondientes certificados son los únicos responsables de su protección y deberían considerar las implicaciones de perder una clave privada de descifrado, dado que puede implicar la pérdida de documentos cifrados.

Dada la existencia de certificados para usos diferentes de la firma electrónica, como la identificación o el cifrado, donde podría resultar confuso el empleo de los términos firmante o persona responsable de los datos de creación de sellos electrónicos de persona jurídica, se emplea el término más genérico de “persona física identificada en el certificado”, siempre con pleno respeto al cumplimiento de la legislación de firma electrónica en relación con los derechos y obligaciones del firmante y de la

persona responsable de los datos de creación de sellos electrónicos de persona jurídica.

1.3.3.4 Partes usuarias

Las partes usuarias son las personas y las organizaciones que reciben firmas digitales y certificados digitales.

Como paso previo a confiar en los certificados, las partes usuarias deben verificarlos, como se establece en esta declaración de prácticas de certificación y en las correspondientes instrucciones de la Autoridad de Certificación.

1.3.4 Otros participantes

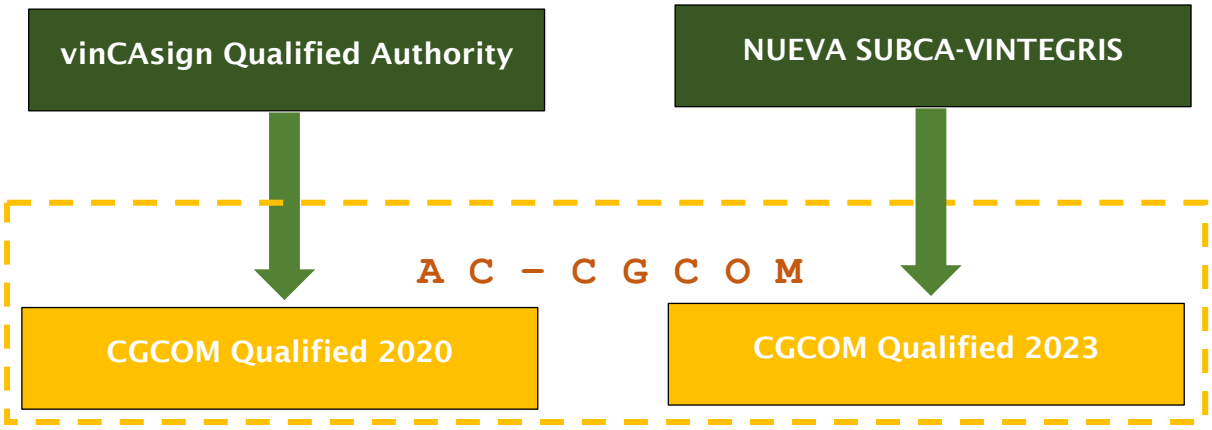
1.3.4.1 Proveedores técnicos

La Autoridad de Certificación del CGCOM se apoya en los servicios de certificación que ofrece su proveedor técnico.

Asimismo, la Autoridad de Certificación del CGCOM se apoya en los servicios de mantenimiento y soporte sobre el producto que ofrece el proveedor técnico "BIT4ID".

1.3.4.2 Jerarquías externas de certificación

La jerarquía de Certificación en la que se integra la Autoridad de Certificación del CGCOM es la siguiente:



1.3.4.2.1 CGCOM QUALIFIED 2020- Autoridad de certificación subordinada

Es la Autoridad de Certificación dentro de la jerarquía que emite los certificados de entidad de los usuarios finales, y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz "vinCAsign Qualified Authority"

En este caso, el proveedor técnico actuará subcontratado para la Autoridad de Certificación del Consejo General de Colegios Oficiales de Médicos (AC-CGCOM).

La AC-CGCOM tiene la siguiente descripción técnica:

Certificate serial: 69:87:AB:7B:34:09:6F:B5:4C:9D:FA:F7:53:B9:1D:BC:FF:3F:9C:F2
Issuer: CN = vinCAsign Qualified Authority, 2.5.4.97 = VATES-B62913926, L = Hospitalet de Llobregat, O = Víntegris SL, S = Barcelona, C = ES
Subject: CN=CGCOM QUALIFIED 2020,OU=ENTIDAD DE CERTIFICACION,organizationIdentifier=VATES-Q2866017C,O=CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS,L=MADRID,ST=MADRID,C=ES
Validity: 02/03/2020 11:41:18 CET - 02/03/2033 11:41:18 CET
Huella digital SHA1: 6F:F9:3A:8C:39:08:F9:F9:A1:7A:B1:76:5E:DF:D2:D6:74:8C:35:A2
Huella digital SHA256: 6E:8A:B9:A7:28:5D:70:EF:22:FC:7D:23:75:83:8D:65:3B:64:87:48:81:7A:80:63:4B:0C:1A:F1:04:3C:D3:66

El OID de la AC-CGCOM es "anypolicy": 2.5.29.32.0

1.3.4.2.2 CGCOM QUALIFIED 2023- Autoridad de certificación subordinada

Es la Autoridad de Certificación dentro de la jerarquía que emite los certificados de entidad de los usuarios finales, y su certificado de clave pública ha sido firmado digitalmente por la Autoridad de Certificación Raíz "CA Vintegris ROOT TrustServices"

En este caso, el proveedor técnico actuará subcontratado para la Autoridad de Certificación del Consejo General de Colegios Oficiales de Médicos (AC-CGCOM).

La AC-CGCOM tiene la siguiente descripción técnica:

Certificate serial: 4ccda5e48417a639b4fa095f9a5c764f9caa9485
Issuer: CN = CA Vintegris ROOT TrustServices, 2.5.4.97 = VATES-B62913926, L = Hospitalet de Llobregat, O = Víntegris SLU, ST = Barcelona, C = ES
Subject: CN=CGCOM QUALIFIED 2023,OU=ENTIDAD DE CERTIFICACION,organizationIdentifier=VATES-Q2866017C,O=CONSEJO GENERAL DE COLEGIOS OFICIALES DE MEDICOS,L=MADRID,ST=MADRID,C=ES
Validity: 24/05/2023 12:25:19 CEST - 21/05/2033 12:25:18 CEST
Huella digital SHA1: 26:4A:34:4F:93:E0:6E:1B:EC:33:5B:7D:24:43:32:67:BF:7C:6B:68
Huella digital SHA256: 87:03:3F:EE:AB:43:12:15:50:5C:DD:79:AE:AF:56:93:36:7D:8B:84:CF:85:34:00:35:A6:A8:B6:92:62:8A:C9

El OID de la AC-CGCOM es “anypolicy”: 2.5.29.32.0

1.4 Uso de los certificados

Esta sección lista las aplicaciones para las que puede emplearse cada tipo de certificado, establece limitaciones a ciertas aplicaciones y prohíbe ciertas aplicaciones de los certificados.

1.4.1 Usos permitidos para los certificados

Se deben tener en cuenta los usos permitidos indicados en los diversos campos de los perfiles de certificados, visibles en el web https://psc.cgcom.es

1.4.1.1 Certificados corporativos de colegiado/a en tarjeta

1.4.1.1.1 Aspectos comunes

Los certificados corporativos de colegiado son certificados 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.

Los certificados corporativos de colegiado 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.

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 y, en consecuencia, es el poseedor de la tarjeta y el software complementario correspondientes.

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.

1.4.1.1.2 Certificado corporativo de colegiado/a para identificación, en tarjeta.

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.1.1
OID política NCP+	0.4.0.2042.1.2

Los certificados corporativos de colegiado (de identificación), en tarjeta, garantizan la identidad de la persona poseedora de la clave privada de identificación, y su vinculación con el suscriptor del servicio de certificación.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas las siguientes funciones:
    a. Digital Signature (para realizar la función de autenticación)
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo “User Notice” nos describe que el uso de este certificado es para la “identificación” del médico colegiado/a”.

1.4.1.1.3 Certificado corporativo de colegiado/a para firma, en tarjeta.

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.1.2
OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de colegiado (de firma) en tarjeta, 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 fima manuscrita.

Por otra parte, los certificados corporativos de colegiado (de firma) se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) 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 puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas las siguientes funciones:
    a. Content commintment (para la realización de la función de firma electrónica)
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "firma electrónica cualificada de médico colegiado/a".

1.4.1.1.4 Certificado de cifrado para colegiado, en tarjeta

OID jerarquía deCGCOM	1.3.6.1.4.1.26852.1.1.1.3

Los certificados de cifrado, en tarjeta, 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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
c) QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

d) El campo "User Notice" nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.2 Certificados corporativos de colegiado centralizados en NUBE

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.1.4
OID política QCP-n-qscd	0.4.0.194112.1.2

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

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 se emiten a colegiados del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

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".

Por otra parte, estos certificados se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación y firma electrónica cualificada del médico colegiado, en nube.

1.4.1.3 Certificados corporativos de colegiado en software

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.1.5
OID política QCP-n	0.4.0.194112.1.0

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

Estos certificados son gestionados en ubicaciones locales del usuario.

Estos certificados no funcionan con dispositivo cualificado de creación de firma

Estos certificados se emiten a colegiados del ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

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

Por otra parte, estos certificados se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

d) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
e) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

f) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación y firma electrónica avanzada del médico colegiado, en software.

1.4.1.4 Certificados corporativos de personas físicas vinculadas en tarjeta

1.4.1.4.1 Aspectos comunes

Los certificados corporativos de persona física vinculada son certificados 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.

Los certificados corporativos de persona física vinculada funcionan con dispositivo seguro 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.

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.

1.4.1.4.2 Certificado corporativo de persona física vinculada para identificación en tarjeta

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.2.1
OID política NCP+	0.4.0.2042.1.2

Los certificados corporativos de persona física vinculada (de identificación) garantizan la identidad de la persona poseedora de la clave privada de identificación, y su vinculación con el suscriptor del servicio de certificación.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
   a. Digital Signature (para realizar la función de autenticación)
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación de persona física vinculada".

1.4.1.4.3 Certificado corporativo de persona física vinculada para firma en tarjeta

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.2.2
OID política QCP-n-qscd	0.4.0.194112.1.2

Los certificados corporativos de persona física vinculada (de firma) 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, tendá un efecto jurídico equivalente al de una fima manuscrita.

Por otra parte, estos certificados se pueden utilizar en aplicaciones que no requieren la firma electrónica equivalente a la firma escrita, como las aplicaciones que se indican a continuación:

a) Firma de correo electrónico seguro.
b) 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 puesto que, al menos, esta firma habrá sido producida con el dispositivo seguro.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Content commintment (para la realización de la función de firma electrónica)
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" nos describe que el uso de este certificado es para la "firma electrónica cualificada de personal administrativo y de servicios".

1.4.1.4.4 Certificado de cifrado de persona física vinculada para cifrado, en tarjeta

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.2.3

Los certificados de cifrado 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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 claves**.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.
c) El campo "User Notice" nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.5 Certificados corporativos de persona física vinculada en NUBE

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.6
OID política QCP-n-qscd	0.4.0.194112.1.2

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

Estos certificados son gestionados de forma centralizada.

Los certificados corporativos de persona física vinculada, emitidos en NUBE, 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.

Los certificados corporativos de persona física vinculada en NUBE, 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, tendá un efecto jurídico equivalente al de una fima manuscrita.

Estos 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.

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".

Por otra parte, los certificados corporativos de persona física vinculada, emitidos en NUBE se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

    a. Firma digital
    b. No repudio

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:

    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación y la firma electrónica cualificada de la persona física vinculada emitido en NUBE".

1.4.1.6 Certificados corporativos de persona física vinculada en software

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.2.5
OID política QCP-n	0.4.0.194112.1.0

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

Estos certificados son gestionados en ubicaciones locales del usuario.

Estos certificados no funcionan con dispositivo cualificado de creación de firma

Estos 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.

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

Por otra parte, estos certificados se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
b) En el campo “Qualified Certificate Statements” aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación y firma electrónica avanzada de la persona física vinculada en software.

1.4.1.7 Sellos electrónicos de persona jurídica

1.4.1.7.1 Aspectos comunes

Los certificados de sello electrónico de persona jurídica son certificados 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.

Estos certificados garantizan la identidad del subscriptor, es decir del Colegio de Médicos u cualquier otra persona jurídica del ámbito sanitario público o privado incluida en el certificado.

1.4.1.7.2 Certificado de sello electrónico de persona jurídica en NUBE

OID jerarquía de la CGCOM	1.3.6.1.4.1.26852.1.1.10.2
OID política QCP-l-qscd	0.4.0.194112.1.3

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.

Estos certificados son gestionados de forma centralizada.

Los certificados de sello electrónico emitido en NUBE, 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.

Los certificados de sello electrónico emitido en NUBE, 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, tendá un efecto jurídico equivalente al de una fima manuscrita.

La AC-CGCOM no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

a) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:
   - Firma digital (para realizar la función de autenticación)
   - Content commintment (para realizar la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   - QcCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" nos describe el uso de este certificado: "CERTIFICADO CUALIFICADO DE SELLO ELECTRONICO PARA LA ACTUACION AUTOMATIZADA, CON USO DE LA CLAVE PRIVADA EXCLUSIVAMENTE CON UN QSCD".

1.4.1.8 Certificados de sello electrónico de persona jurídica en software

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.10.5
OID política QCP-l	0.4.0.194112.1.1

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

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

Estos certificados no funcionan con dispositivo cualificado 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.

Por otra parte, estos certificados se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

d) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
e) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

f) El campo "User Notice" nos describe que el uso de este certificado es para el " sellado electrónico para la actuación automatizada en software.

1.4.1.9 Certificados corporativo de Representante de Persona Jurídica en tarjeta

1.4.1.9.1 Aspectos comunes

Los certificados corporativos de Representante de PJ son certificados 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.

Los certificados corporativos de Representante de PJ funcionan con dispositivo seguro 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.

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), y 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.

1.4.1.9.2 Certificado corporativo de representante de PJ para identificación

OID jerarquía del CGCOM	1.3.6.1.4.1.26852.1.1.11.1
OID política NCP+	0.4.0.2042.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
   a. Digital Signature (para realizar la función de autenticación)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

1.4.1.1.2 Certificado corporativo de representante de PJ, para firma

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.11.2
OID política QCP-n-qscd	0.4.0.194112.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

Los certificados corporativos de representante de PJ (de firma) 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.

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.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:

   a. Content commintment (para la realización de la función de firma electrónica)

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:

   - qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
   - QcSSCD (0.4.0.1862.1.4), que informa que el certificado se u sa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

1.4.1.1.3 Certificado de cifrado de representante de PJ, en tarjeta

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.11.3
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

Los certificados de cifrado 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 de la persona física indicada en el certificado.
b) Una clave de cifrado de sesión, simétrica, cifrada con la clave pública de la persona física indicada en el certificado.

En todo caso, esta persona física deberá utilizar su clave privada para descifrar el mensaje, advirtiéndose al suscriptor del servicio y a dicha persona 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 claves.

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Key Encipherment

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.
    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo seguro de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la función de cifrado.

1.4.1.2 Certificados corporativos de Representante de Persona Jurídica en NUBE

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.12

OID política QCP-n-QSCD	0.4.0.194112.1.2
OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

Los certificados corporativos de representante emitidos en NUBE, son certificados 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.

Los certificados corporativos de representante emitido en NUBE, 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.

Los certificados corporativos de representante emitido en NUBE, 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.

Estos certificados se emiten a representantes de persona jurídica, en el ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

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".

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

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

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo "key usage" tiene activadas y por tanto nos permite realizar, las siguientes funciones:
    a. Firma digital
    b. No repudio
b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:

    a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

    b. QcSSCD (0.4.0.1862.1.4), que informa que el certificado se usa exclusivamente en conjunción con un dispositivo cualificado de creación de firma.

c) El campo "User Notice" nos describe que el uso de este certificado es para la ""CERTIFICADO CUALIFICADO DE REPRESENTANTE PJ, EN NUBE"".

1.4.1.10 Certificados corporativos de persona física representante en software

OID jerarquía de CGCOM	1.3.6.1.4.1.26852.1.1.11.5
OID política QCP-n	0.4.0.194112.1.0

OID política representante de persona jurídica, con poderes totales, administrador único o solidario de la organización, o al menos con poderes específicos generales para actuar ante las Administraciones Públicas españolas	2.16.724.1.3.5.8

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

Estos certificados son gestionados en ubicaciones locales del usuario.

Estos certificados no funcionan con dispositivo cualificado de creación de firma

Estos certificados se emiten a representantes de personas jurídicas en el ámbito corporativo del colegio suscriptor, y no son emitidos al público en ningún caso.

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

Por otra parte, estos certificados se pueden utilizar en otras aplicaciones como las que se indican a continuación:

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

La información de usos en el perfil de certificado nos indica lo siguiente:

a) El campo “key usage” tiene activadas y por tanto nos permite realizar, las siguientes funciones:

a. Firma digital
b. No repudio

b) En el campo "Qualified Certificate Statements" aparece la siguiente declaración:
   a. qCCompliance (0.4.0.1862.1.1), que informa que el certificado se emite como cualificado.

c) El campo "User Notice" nos describe que el uso de este certificado es para la "identificación y firma electrónica avanzada de la persona física vinculada en software.

1.4.1.11 Certificados no cualificados de sellos electrónicos de persona jurídica

Estos certificados garantizan la identidad del subscriptor, es decir del Colegio de Médicos u cualquier otra persona jurídica del ámbito sanitario público o privado incluida en el certificado.

OID jerarquía de la CGCOM	1.3.6.1.4.1.26852.1.100.10.1
OID política NCP	0.4.0.2042.1.1

Estos certificadosdan cumplimiento a lo dispuesto por la normativa técnica identificada con la referencia ETSI EN 319 411-1.

Estos certificados emitidos en software, permiten la generación de "sellos electrónicos".

La AC-CGCOM no responderá por pérdida alguna de información cifrada que no se pueda recuperar.

La información de usos en el perfil de certificado indica lo siguiente:

d) El campo "key usage" tiene activadas, y por tanto nos permite realizar, las siguientes funciones:

- Firma digital (para realizar la función de autenticación)
- Content commintment (para realizar la función de firma electrónica)
- Key Encipherment (para la función de cifrado)

e) El campo "User Notice" nos describe el uso de este certificado: ""CERTIFICADO DE SELLO ELECTRONICO DE PERSONA JURIDICA EN SOFTWARE".

1.4.2 Límites y prohibiciones de uso de los certificados

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 (CRL).

Los certificados no se han diseñado, no se pueden destinar y no se autoriza su uso o reventa, sin estar limitado a los siguientes: 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; sistemas de control de armamento; sistemas de gestión y control de aparatos médicos, 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 https://psc.cgcom.es

El empleo de los certificados digitales en operaciones que contravienen la Política de Certificación, esta DPC, los documentos jurídicos vinculantes con cada certificado o los Contratos o Convenios con las entidades de Registro o con sus Firmantes/Suscriptores tiene la consideración de usos indebidos, a los efectos legales oportunos, eximiéndose por tanto la Autoridad de Certificación, en función de la

legislación vigente, de cualquier responsabilidad por este uso indebido de los certificados que realice el firmante o cualquier tercero.

La Autoridad de Certificación 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, el firmante o la persona responsable de la custodia cualquier responsabilidad que pudiese derivarse de la utilización del mismo fuera de los límites y condiciones de uso recogidas en la Política de Certificación, esta DPC, los documentos jurídicos vinculantes con cada certificado o los Contratos o Convenios con las entidades de Registro o con sus 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.

1.5 Administración de la política

1.5.1 Organización que administra el documento

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

1.5.2 Datos de contacto de la organización

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

1.5.3 Procedimientos de gestión del documento

El sistema documental y de organización de la Autoridad de Certificación del CGCOM garantiza, mediante la existencia y la aplicación de los correspondientes procedimientos, el correcto mantenimiento de este documento y de las especificaciones de servicio relacionados con el mismo.

1.5.3.1 REVISIÓN DEL DOCUMENTO

El CGCOM revisa esta Declaración de Prácticas de Confianza una vez al año como mínimo.

La Comisión Permanente será el responsable del mantenimiento de este documento siguiendo las directrices de la Política de seguridad y del procedimiento asociado.

El *Responsable de Seguridad* propone cambios y recoge sugerencias y propuestas para su estudio y envío al *Comité de Seguridad* para su aprobación.

El *Comité de Seguridad* avaluará la necesidad que los cambios propuestos requieran de notificación ante al supervisor.

Fases de seguimiento de los cambios:

1. Fase A: Recogida de sugerencias y propuestas
2. Fase B: Estudio, análisis, comprobación y redacción
3. Fase C: Envío al *Comité de Seguridad* para comentarios, redacción final y aprobación.
4. Fase D: Publicación en la web, y si fuera requerido notificación al supervisor.

El CGCOM realiza una nueva revisión de esta DPC ante la inclusión de cambios suficientemente relevantes para la gestión de los servicios de certificación. La descripción de los cambios se incluirán en el apartado "control de versiones" de la sección "Información General" en el inicio de este documento.

1.5.3.2 APROBACIÓN DEL DOCUMENTO

Las modificaciones futuras de esta Declaración de Prácticas de Confianza, de la *Política de Seguridad* y de los Textos de Divulgación (PDS) son aprobadas por la Comisión Permanente, siendo el Comité de Seguridad el responsable de su correcta implementación.

El CGCOM comunica de forma permanente los cambios que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en su web https://psc.cgcom.es

1.6 Definiciones y acrónimos

1.6.1 Definiciones

Autoridad de Certificación	Es la entidad responsable de la emisión y gestión de los certificados digitales.
Autoridad de Registro	Entidad responsable de la gestión de las solicitudes, identificación y registro de los solicitantes de un certificado. Puede formar parte de la Autoridad de Certificación o ser ajena.
Certificado	Archivo que asocia la clave pública con algunos datos identificativos del Sujeto/Firmante y es firmada por la AC.

Clave pública	Valor matemático conocido públicamente y usado para la verificación de una firma digital o el cifrado de datos.
Clave privada	Valor matemático conocido únicamente por el Sujeto/Firmante y usado para la creación de una firma digital o el descifrado de datos. La clave privada de la AC será usada para la firma de certificados y firma de CRL's.
DPC	Conjunto de prácticas adoptadas por una Autoridad de Certificación para la emisión de certificados en conformidad con una política de certificación concreta.
CRL	Archivo que contiene una lista de los certificados que han sido revocados en un periodo de tiempo determinado y que es firmada por la AC.
Datos de Activación	Datos privados, como PIN's o contraseñas empleados para la activación de la clave privada
DCCF	Dispositivo Cualificado de creación de firma. Elemento software o hardware, convenientemente certificado, empleado por el Sujeto/Firmante para la generación de firmas electrónicas, de manera que se realicen las operaciones criptográficas dentro del dispositivo y se garantice su control únicamente por el Sujeto/Firmante.
Firma digital	El resultado de la transformación de un mensaje, o cualquier tipo de dato, por la aplicación de la clave privada en conjunción con unos algoritmos conocidos, garantizando de esta manera: a) que los datos no han sido modificados (integridad) b) que la persona que firma los datos es quien dice ser (identificación)

	a) c) que la persona que firma los datos no puede negar haberlo hecho (no repudio en origen)
OID	Identificador numérico único registrado bajo la estandarización ISO y referido a un objeto o clase de objeto determinado.
Par de claves	Conjunto formado por la clave pública y privada, ambas relacionadas entre sí matemáticamente.
PKI	Conjunto de elementos hardware, software, recursos humanos, procedimientos, etc., que componen un sistema basado en la creación y gestión de certificados de clave pública.
Solicitante	En el contexto de este documento, el solicitante será una persona física apoderada con un poder especial para realizar determinados trámites en nombre y representación de una persona jurídica.
Suscriptor	En el contexto de este documento la persona jurídica propietaria del certificado (a nivel corporativo).
Sujeto/Firmante	En el contexto de este documento, la persona física cuya clave pública es certificada por la AC y dispone de, o tiene acceso de forma exclusiva a, una clave privada válida para generar firmas digitales.
Parte Usuaria	En el contexto de este documento, persona que voluntariamente confía en el certificado digital y lo utiliza como medio de acreditación de la autenticidad e integridad del documento firmado

1.6.2 Acrónimos

AC (*o también CA*)	*Certificate Authority* Autoridad de Certificación
AR (o también RA)	*Registration Authority* Autoridad de Registro
CPD	Centro de Proceso de Datos
DPC (o también CPS)	*Certification Practice Statement.* Declaración de Prácticas de Certificación
CRL (o tambien LRC)	*Certificate Revocation List.* Lista de certificados revocados
DN	*Distinguished Name.* Nombre distintivo dentro del certificado digital
DNI	Documento Nacional de Identidad
ETSI EN	*European Telecommunications Standards Institute – European Standard.*
FIPS	*Federal Information Processing Standard Publication*
HSM	*Hardware Security Module* Módulo de seguridad en Hardware
IETF	*Internet Engineering Task Force*
NIF	Número de Identificación Fiscal

NTP	*Network Time Protocol* Protocolo de tiempo en red.
OCSP	*On-line Certificate Status Protocol.* Protocolo de acceso al estado de los certificados
OID	*Object Identifier.* Identificador de objeto
PDS	*PKI Disclosure Statements* Texto de Divulgación de PKI.
PIN	*Personal Identification Number.* Número de identificación personal
PKI	*Public Key Infrastructure.* Infraestructura de clave pública
QSCD (o también DCCF)	*Qualified Electronic Signature/Seal Creation Device.* Dispositivo cualificado de creación de firma/sellos
QCP	*Qualified Certificate Policy* Política de certificados cualificados
QCP-n	*Policy for EU qualified certificate issued to a natural person* Política de certificados cualificados para personas físicas.
QCP-l	*Policy for EU qualified certificate issued to a legal person* Política de certificados cualificados para personas jurídicas.

QCP-n-qscd	*Policy for EU qualified certificate issued to a natural person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas físicas con dispositivo cualificado de firma/sello
QCP-l-qscd	*Policy for EU qualified certificate issued to a legal person where the private key and the related certificate reside on a QSCD* Política de certificados cualificados para personas jurídicas con dispositivo cualificado de firma/sello
RFC	*Request for Comments* Documento RFC
RSA	Rivest-Shimar-Adleman. Tipo de algoritmo de cifrado
SHA	*Secure Hash Algorithm.* Algoritmo seguro de Hash
SSL	*Secure Sockets Layer.* Protocolo diseñado por Netscape y convertido en estándar de la red, permite la transmisión de información cifrada entre un navegador de Internet y un servidor.
TCP/IP	*Transmission Control. Protocol/Internet Protocol.* Sistema de protocolos, definidos en el marco de la IEFT.

TSA	*Time Stamping Authority* Autoridad de Sellado de Tiempo Electrónico
TSU	*Time Stamping Unit* Unidad de Sellado de Tiempo.
UTC	*Coordinated Universal Time* Tiempo universal coordinado
VPN	*Virtual Private Network.* Red privada virtual

2 Publicación de información y depósito de certificados

2.1 Depósito(s) de certificados

La Autoridad de Certificación del CGCOM dispone de un Depósito de certificados, en el que se publican las informaciones relativas a los servicios de certificación.

Dicho servicio se encuentra disponible durante las 24 horas de los 7 días de la semana y, en caso de fallo del sistema fuera de control de la Autoridad de Certificación del CGCOM, ésta realizará sus mejores esfuerzos para que el servicio se encuentre disponible de nuevo en el plazo establecido en la sección 5.7.4 de esta Declaración de Prácticas de Certificación.

2.2 Publicación de información del prestador de servicios de certificación

La Autoridad de Certificación del CGCOM publica las siguientes informaciones, en su Depósito:

- Los certificados emitidos, cuando se haya obtenido consentimiento de la persona física identificada en el certificado.
- Las listas de certificados revocados y otras informaciones de estado de revocación de los certificados.
- Las políticas de certificados aplicables.
- La Declaración de Prácticas de Certificación, en lengua española.
- Los textos de divulgación (PKI Disclosure Statements – PDS), en lengua española.

2.3 Frecuencia de publicación

La información del prestador de servicios de certificación, incluyendo las políticas y la Declaración de Prácticas de Certificación, se publica en cuanto se encuentra disponible.

Los cambios en la Declaración de Prácticas de Certificación se rigen por lo establecido en la sección 1.5 de este documento.
La información de estado de revocación de certificados se publica de acuerdo con lo establecido en las secciones 4.9.7 y 4.9.8 de esta Declaración de Prácticas de Certificación.

2.4 Control de acceso

La Autoridad de Certificación del CGCOM no limita el acceso de lectura a las informaciones establecidas en la sección 2.2, pero establece controles para impedir que personas no autorizadas puedan añadir, modificar o borrar registros del Depósito, para proteger la integridad y autenticidad de la información, especialmente la información de estado de revocación.

La Autoridad de Certificación emplea sistemas fiables para el Depósito, de modo tal que:

- Únicamente personas autorizadas puedan hacer anotaciones y modificaciones.
- Pueda comprobarse la autenticidad de la información.
- Los certificados sólo estén disponibles para consulta si la persona física identificada en el certificado ha prestado su consentimiento.
- Pueda detectarse cualquier cambio técnico que afecte a los requisitos de seguridad.

3 Identificación y autenticación

3.1 Registro inicial

3.1.1 Tipos de nombres

Todos los certificados contienen un nombre diferenciado X.501 en el campo *Subject*, incluyendo un componente *Common Name* (CN=), relativo a la identidad del suscriptor y de la persona física identificada en el certificado, así como diversas informaciones de identidad adicionales en el campo *SubjectAlternativeName*.

Los nombres contenidos en los certificados son los siguientes.

3.1.1.1 *Certificado corporativo de colegiado/a (Tarjeta, NUBE,soft)*

Country (C)	"ES"
Organization (O)	Colegio profesional
Surname	Apellidos
Given Name	Nombre
Title	"Médico colegiado/a"
Serial Number	DNI/NIE, en formato ETSI
Common Name (CN)	Nombre, apellidos y número del DNI/NIE
DirectoyName:	
OID.1.3.6.1.4.1.26852.2.9	Nombre de la persona física
OID.1.3.6.1.4.1.26852.2.10	Apellido primero de la persona física
OID.1.3.6.1.4.1.26852.2.11	Apellido segundo de la persona física
OID.1.3.6.1.4.1.26852.2.12	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")

3.1.1.2 *Certificado corporativo de persona física vinculada (Tarjeta, NUBE, soft)*

Country (C)	"ES"
Organization (O)	Colegio profesional
Surname	Apellidos

Given Name	Nombre
Title	Cargo persona física
Serial Number	DNI/NIE, en formato ETSI
DirectoyName:	
OID.1.3.6.1.4.1.26852.2.9	Nombre de la persona física
OID.1.3.6.1.4.1.26852.2.10	Apellido primero de la persona física
OID.1.3.6.1.4.1.26852.2.11	Apellido segundo de la persona física
OID.1.3.6.1.4.1.26852.2.12	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")

3.1.1.3 Certificado corporativo de Representante legal (Tarjeta, NUBE, soft)

Country (C)	"ES"
Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario
Surname	Apellidos
Given Name	Nombre
Serial Number	DNI/NIE del representante, en formato ETSI
Common Name (CN)	DNI Representante legal, nombre y apellidos, NIF del Colegio o PJ representada.
DirectoyName:	
OID.1.3.6.1.4.1.26852.2.9	Nombre de la persona física
OID.1.3.6.1.4.1.26852.2.10	Apellido primero de la persona física
OID.1.3.6.1.4.1.26852.2.11	Apellido segundo de la persona física
OID.1.3.6.1.4.1.26852.2.12	NIF del titular acorde a ETSI EN 319 412-1 "IDCES-123456789Z")

3.1.1.4 Certificado corporativo de Sello electrónico (NUBE, soft)

Country (C)	"ES"
Organization (O)	Colegio profesional u otra persona jurídica del ámbito sanitario
Serial Number	NIF de la persona jurídica

3.1.2 Significado de los nombres

Los nombres contenidos en los campos *SubjectName* y *SubjectAlternativeName* de los certificados son comprensibles en lenguaje natural y serán interpretados de acuerdo con la legislación española aplicable a los nombres de las personas físicas y jurídicas.

3.1.3 Empleo de anónimos y seudónimos

En general no se pueden utilizar seudónimos para identificar una organización.

Se pueden utilizar seudónimos en certificados personales siempre que en caso necesario se pueda determinar su identidad.

En ningún caso se emiten certificados de anónimos.

3.1.4 Interpretación de formatos de nombres

Los formatos de nombres se interpretarán de acuerdo con la ley española, en sus propios términos.

El campo "país" siempre será España, dado que el certificado muestra la relación entre un colegiado, una persona física vinculada o un representante legal y un colegio profesional español, con independencia de la nacionalidad del colegiado, persona física vinculada o representante legal. Ello deriva de la naturaleza corporativa del certificado, del cual es suscriptor el colegio, y, el colegiado, persona física vinculada o representante legal la persona autorizada a su uso.
El campo "número de serie" debe incluir el DNI o el NIE del colegiado, persona física vinculada, representante legal o médico empleado público al efecto de la admisión del certificado para la realización de trámites con las Administraciones españolas.

3.1.5 Unicidad de los nombres

Los nombres de los suscriptores de certificados serán únicos, para cada política de certificado de la Autoridad de Certificación del CGCOM.

No se podrá asignar un nombre de suscriptor que ya haya sido empleado, a un suscriptor diferente, situación que, en principio no se ha de dar, gracias a la presencia del número del Documento Nacional de Identidad, o equivalente, en el esquema de nombres.

Un suscriptor puede pedir más de un certificado siempre que la combinación de los siguientes valores existentes en la solicitud fuera diferente de un certificado válido:

- Número de Identificación Fiscal (NIF) de la persona física
- Código de Identificación Fiscal (CIF) del colegio de médicos o persona jurídica del ámbito sanitario.
- Tipo de Certificado (Campo descripción del certificado).

3.1.6 Resolución de conflictos relativos a nombres

Los solicitantes de certificados no incluirán nombres en las solicitudes que puedan suponer infracción, por el futuro suscriptor, de derechos de terceros.

La Autoridad de Certificación del CGCOM no estará obligada a determinar previamente que un solicitante de certificados tiene derecho sobre el nombre que aparece en una solicitud de certificado, sino que en principio procederá a certificarlo.

Asimismo, no actuará como árbitro o mediador, ni de ningún otro modo deberá resolver disputa alguna concerniente a la propiedad de nombres de personas u organizaciones, nombres de dominio, marcas o nombres comerciales.

Sin embargo, en caso de recibir una notificación relativa a un conflicto de nombres, conforme a la legislación española, podrá emprender las acciones pertinentes orientadas a bloquear o retirar el certificado emitido.

En todo caso, el prestador de servicios de certificación se reserva el derecho de rechazar una solicitud de certificado debido a conflicto de nombres.

Toda controversia o conflicto que se derive del presente documento, se resolverá definitivamente, mediante el arbitraje de derecho de un árbitro, en el marco de la Corte Española de Arbitraje, de conformidad con su Reglamento y Estatuto, a la que

se encomienda la administración del arbitraje y la designación del árbitro o tribunal arbitral. Las partes hacen constar su compromiso de cumplir el laudo que se dicte.

3.2 Validación inicial de la identidad

La identidad de los suscriptores de certificados corporativos, son las entidades que integran la Consejo General de Colegios Oficiales de Médicos u otras entidades jurídicas del ámbito sanitario, resulta fijada de antemano, y la identidad de las personas físicas identificadas en dichos certificados corporativos – colegiados/as, , representantes de persona jurídica y personal vinculado – se valida mediante los registros corporativos de la entidad.

La identidad de los suscriptores en otras entidades jurídicas del ámbito sanitario resulta fijada de antemano. Será necesario disponer para los servicios de certificación digital de un convenio entre la CGCOM y estas entidades. La identificación de los trabajadores de estas entidades se validan mediante sus registros internos y la identidad como médicos se valida mediante los registros del CGCOM.

A estos efectos, el Consejo General de Colegios Oficiales de Médicos dispone de un sistema de registro que garantiza la corrección y consistencia de las informaciones contenidas en dichos registros corporativos.

En relación a los datos personales de cada entidad, empresa u organización de derecho público o privado, AC-CGCOM actúa como encargado del tratamiento en los términos indicados en al apartado 9.4 de este documento.

3.2.1 Prueba de posesión de clave privada

El par de claves es generado por la Autoridad de Certificación de CGCOM, en su caso asistido por las entidades indicadas en la sección 1.3.4.1 de esta Declaración de Prácticas de Certificación, por delegación del solicitante, durante el proceso de personalización final del dispositivo seguro de creación de firma del suscriptor.

En este caso, la posesión de la clave privada se demuestra en virtud del procedimiento fiable de entrega y aceptación del certificado y, cuando corresponda, del correspondiente dispositivo seguro y par de claves almacenados en su interior.

3.2.2 Autenticación de la identidad de una organización

3.2.2.1 Colegios de Médicos y CGCOM

No se requiere realizar procedimiento de autenticación de la existencia de la organización titular del certificado en certificados corporativos, dado que la organización forma parte del ámbito corporativo del Consejo General de Colegios Oficiales de Médicos y por tanto se encuentra fijada de antemano.

La identidad de los Colegio Oficiales de Médicos

La Ley 2/1974, de 13 de febrero, de Colegios Profesionales, indica en su artículo 1.1 que "*los Colegios Profesionales son Corporaciones de derecho publico, amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines*". Asimismo, su artículo 1.3, en redacción dada por Ley 25/2009, de 22 de diciembre, establece que "*son fines esenciales de estas Corporaciones la ordenación del ejercicio de las profesiones, la representación institucional exclusiva de las mismas cuando estén sujetas a colegiación obligatoria, la defensa de los intereses profesionales de los colegiados y la protección de los intereses de los consumidores y usuarios de los servicios de sus colegiados, todo ello sin perjuicio de la competencia de la Administración Pública por razón de la relación funcionarial*".

La Ley 2/1974 establece en su artículo 4.1 que "*la creación de Colegios Profesionales se hará mediante Ley, a petición de los profesionales interesados[…]*" y, en su apartado 4, que "*cuando estén constituidos varios Colegios de la misma profesión de ámbito inferior al nacional existirá un Consejo General cuya naturaleza y funciones se precisan en el artículo noveno*".

La identidad del Consejo General de Colegios Oficiales de Médicos.

El artículo 9.1 de la Ley 2/1974 indica que "*Los Consejos Generales de los Colegios tienen a todos los efectos la condición de Corporación de Derecho público, con personalidad jurídica propia y plena capacidad. Tendrán las siguientes funciones*:

[…]
b) Elaborar los Estatutos generales de los Colegios, así como los suyos propios.
c) aprobar los Estatutos y visar los Reglamentos de régimen interior de los Colegios.
d) Dirimir los conflictos que puedan suscitarse entre los distintos Colegios.
e) Resolver los recursos que se interpongan contra los actos de los Colegios.
f) Adoptar las medidas necesarias para que los Colegios cumplan las resoluciones del propio Consejo Superior dictadas en materia de su competencia.
g) Ejercer las funciones disciplinarias con respecto a los miembros de las Juntas de Gobierno de los Colegios y del propio Consejo.
[…]"

La disposición adicional tercera de la Ley 2/1974, indica que "*1. Se entiende por organización colegial el conjunto de corporaciones colegiales de una determinada profesión. 2. Son corporaciones colegiales el Consejo General o Superior de Colegios, los Colegios de ámbito estatal, los Consejos Autonómicos de Colegios y los Colegios Profesionales*".

Los Estatutos del Consejo General de Colegios Oficiales de Médicos, aprobados por Real Decreto 300/2016, de 22 de julio, indican en su artículo 1 que "*El Consejo General de Colegios Oficiales de Médicos, Corporación de derecho público con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, agrupa, coordina y representa a todos los Colegios Oficiales de Médicos a nivel estatal*".

El artículo 2 indica "*1. Con carácter general, corresponden al Consejo General de Colegios Oficiales de Médicos las funciones previstas en la normativa sobre Colegios Profesionales. 2. Asimismo, le corresponden las siguientes funciones: a) Ostentar la representación de la Organización Médica Colegial ante todas las organizaciones médicas y sanitarias internacionales. b) Representar a la Organización Médica Colegial ante las instituciones de la Unión Europea en aquellos temas que afecten al ejercicio profesional y a sus aspectos éticos y deontológicos*".

El artículo 4 establece que:"*La Asamblea General es el máximo órgano rector del Consejo General y estará integrada por los siguientes miembros:*

a) Las Presidencias de los Colegios Oficiales de Médicos.
b) Los miembros de la Comisión Permanente.
c) Los Representantes Nacionales de las Secciones Colegiales que, de conformidad con las disposiciones estatutarias, estén constituidas.
d) Los representantes de la Universidad, de las Sociedades Científicas y de otras entidades médicas que, con voz pero sin voto,la propia Asamblea acuerde incorporar.

Por su parte, el artículo 20 de dichos estatutos establece que "*Corresponde a la Presidencia: a) Ostentar la representación máxima del Consejo General, estándole asignado el ejercicio de cuantos derechos y funciones le atribuyan la Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales, y los Estatutos del Consejo General en todas las relaciones con los poderes públicos, entidades, corporaciones y personas jurídicas o naturales de cualquier orden, siempre que se trate de materias de interés general para la profesión. b) Ejercitar las acciones que correspondan en defensa de los derechos e intereses de la Corporación y de la profesión ante los órganos jurisdiccionales, administrativos e institucionales de toda clase*", en sentido análogo al artículo 7.4 de la Ley 2/1974.

3.2.2.2 Sociedades profesionales

La identificación para la expedición de certificados de persona jurídica a Sociedades profesionales queda garantizada por el registro correspondiente en cada Colegio de Médicos. La Ley 44/2003, de 21 de noviembre, de ordenación de las profesiones sanitarias, en su artículo 5.2 establece que "*para garantizar de forma efectiva y facilitar el ejercicio de los derechos a que se refiere el apartado anterior, los colegios profesionales, consejos autonómicos y consejos generales, en sus respectivos ámbitos territoriales, establecerán los registros públicos de profesionales que, de acuerdo con los requerimientos de esta ley, serán accesibles a la población y estarán a disposición de las Administraciones sanitarias […]*".

3.2.2.3 Fundaciones

No se requiere realizar procedimiento de autenticación de la existencia de cada una de las fundaciones titulares del certificado en certificados corporativos, dado que dichas fundaciones forman parte del ámbito corporativo Consejo General de Colegios Oficiales de Médicos y por tanto se encuentra fijada de antemano.

La identidad de las Fundaciones Consejo General de Colegios Oficiales de Médicos

La Ley 50/2002, de 26 de diciembre, de Fundaciones, indica en su artículo 2 que "*Son fundaciones las organizaciones constituidas sin fin de lucro que, por voluntad de sus creadores, tienen afectado de modo duradero su patrimonio a la realización de fines de interés general. Las fundaciones se rigen por la voluntad del fundador, por sus Estatutos y, en todo caso, por la Ley.*"

Asimismo, el artículo 4 de dicho texto legal establece, en relación a la personalidad jurídica de las mismas, *que "dispondrán de ella desde la inscripción de la escritura pública de su constitución en el correspondiente Registro de Fundaciones. La inscripción sólo podrá ser denegada cuando dicha escritura no se ajuste a las prescripciones de la Ley".*

El Consejo General de Colegios Oficiales de Médicos dispone de 3 fundaciones en el seno de su ámbito corporativo, lo cual se observa de los estatutos que las regulan:

- ***Fundación patronato de huérfanos y protección social de médicos "Príncipe de Asturias***", cuyos estatutos disponen:

  "Artículo 1º. Denominación y naturaleza. Bajo la denominación de "FUNDACIÓN PATRONATO DE HUÉRFANOS Y PROTECCIÓN SOCIAL DE MÉDICOS "PRINCIPE DE ASTURIAS" se constituye una Fundación de interés general y carácter particular, organización privada sin ánimo de lucro bajo el patrocinio del Consejo General de Colegios Médicos, que estará tutelada por el Protectorado que actualmente desempeña el Ministerio de Trabajo y Asuntos Sociales.

Artículo 2º. Personalidad y capacidad. La Fundación está inscrita en el Registro de Fundaciones, tiene personalidad jurídica propia y plena capacidad de obrar, a tenor de lo dispuesto en el artículo 35 del Código Civil, pudiendo en consecuencia realizar todos aquellos actos que sean necesarios para el cumplimiento de los fines para los que ha sido creada, con sujeción a lo establecido en el Ordenamiento Jurídico."

- ***Fundación red de colegios médicos solidarios***, cuyos estatutos disponen:

  "Artículo 2.- Personalidad y capacidad. La Fundación constituida, una vez inscrita en el Registro de Fundaciones, tiene personalidad jurídica propia y plena capacidad para obrar, pudiendo realizar, en consecuencia, todos aquellos actos que sean necesarios para el cumplimiento de la finalidad para la que ha sido creada, con sujeción a lo establecido en el ordenamiento jurídico."

  "Art. 11.- Naturaleza del Patronato y de la Junta Rectora.
  El órgano de gobierno, representación y administración de la Fundación es el Patronato, por tanto, la Junta Rectora actuará dentro de las limitaciones legales y siempre por delegación de facultades del mismo. Su mandato será el equivalente al del cargo que desempeñen como miembros de la Asamblea General del Consejo General de Colegios Oficiales de Médicos. Finalizado su mandato se convocarán elecciones para cubrir los cargos de patronos que quedaron vacantes."

- ***Fundación para la Formación de la OMC (FFOMC)***, cuyos estatutos disponen:

  "Artículo 21 . - El Patronato es el órgano supremo de gobierno, administración y representación de la Fundación: Serán miembros natos del Patronato los siguientes:
  - *Presidente. Que será el que obtenga igual cargo en el Consejo Oficial de Médicos.*
  - *Vicepresidente. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.*

- *Secretario. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.*
- *Vicesecretario. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.*
- *Tesorero. Que será el que ostente igual cargo en el Consejo Oficial de Médicos.*
- *Serán igualmente miembros de Patronato 5 Vocales designados por elección de entre y por los miembros que integran la Asamblea General de la O.M.C.*

El Patronato podrá acordar por unanimidad el nombramiento de otros miembros, en función de los intereses funcionales, cuya duración en el cargo se hará coincidir con el del Presidente del Patronato. La duración del cargo de los miembros natos del Patronato, será la del cargo que se ocupen en el momento de acceder a la Asamblea General de Colegios Oficiales de Médicos. El Presidente tendrá voto de calidad."

3.2.2.4 Otras entidades jurídicas del ámbito sanitario

No se requiere realizar procedimiento de autenticación de la existencia de otras entidades jurídicas del ámbito sanitario, dado que se encuentra fijada de antemano.

Se define a estas entidades jurídicas del ámbito sanitario como a aquellas entidades donde se ofrecen un conjunto de servicios que se proporcionan al individuo, con el fin de promover, proteger y restaurar su salud, donde tienen cabida la prevención, el tratamiento y el manejo de la enfermedad y la preservación del bienestar mental y físico a través de los servicios ofrecidos por los profesionales médicos y afines.

La existencia de estas entidades jurídicas del ámbito sanitario (como Hospitales, Clínicas, Centros de Salud, etc.) le consta al Consejo General de Colegios Oficiales de Médicos por su relación institucional permanente y por la relación laboral de muchos de sus miembros –los médicos colegiados en los Colegios Oficiales de Médicos- con dichas entidades jurídicas del ámbito sanitario.

La prestación del servicio de certificación digital se formaliza mediante el oportuno convenio de colaboración entre la Autoridad de Certificación del CGCOM y cada una de estas entidades jurídicas del ámbito sanitario.

3.2.2.5 Para todos los casos

Se comprueban, la autorización del solicitante de certificados y la existencia del dominio de correo electrónico corporativo.

3.2.3 Autenticación de la identidad de una persona física

Esta sección describe los métodos de comprobación de la identidad de una persona física identificada en un certificado.

3.2.3.1 En certificados corporativos

Los registros colegiales, que se integran en el Sistema de Registro son los únicos que legalmente permiten acreditar la condición de médico colegiado/a.
Los datos de los órganos colegiales y del personal administrativo se encuentran en otros registros colegiales.
Por este motivo, la información de identificación de las personas físicas identificadas en los certificados corporativos se valida comparando la información de la solicitud con los registros del Colegio correspondiente, asegurando la corrección de la información a certificar.

3.2.3.2 Necesidad de presencia personal

En general, no se requiere presencia física para la solicitud de certificados, ya que la solicitud se realiza empleando los datos incluidos en los registros profesionales, que se mantienen permanentemente actualizados.

Sin embargo, antes de la entrega de un certificado de firma electrónica, la Autoridad de Certificación del CGCOM deberá verificar la identidad de la persona física identificada en el certificado mediante cualquiera de los siguientes sistemas:

- Verificación en presencia física. Durante este trámite, que se realiza con la colaboración del Colegio o de la organización del ámbito sanitario solicitante, se confirma fehacientemente la identidad de la persona física identificada en

el certificado, en los términos previstos en el artículo 24.1 del Reglamento (UE) 910/2014 y el artículo 7 de la Ley 6/2020.

- Verificación a distancia, utilizando medios de identificación electrónica, para los cuales se haya garantizado la presencia de la persona física, y que cumplan los requisitos establecidos con el artículo 8 con respecto a los niveles de seguridad «sustancial» o «alto». En particular, resulta admisible el DNI electrónico. Si el medio de identificación electrónica incorpora capacidades de firma electrónica avanzada o cualificada, se podrá emplear para la firma de la hoja de aceptación.
- Verificación a distancia, por medio de un certificado de una firma electrónica cualificada expedido de conformidad con los puntos anteriores. En este caso, se utilizará la firma electrónica cualificada para la firma de la hoja de aceptación

Esta presencia personal en la solicitud de certificados no será necesaria si la firma de la hoja de solicitud y aceptación del certificado ha sido legitimada ante notario.

3.2.3.3 Vinculación de la persona física con una organización

La justificación documental de la vinculación de una persona física identificada en un certificado con el Colegio, la organización del ámbito sanitario es la propia solicitud y su presencia en el registro de médicos del Colegio (para colegiados) o en otros registros internos (para las personas física vinculadas).

3.2.4 Información de suscriptor no verificada

La Autoridad de Certificación del CGCOM no incluye ninguna información de suscriptor no verificada en los certificados.

3.3 Identificación y autenticación de solicitudes de renovación

3.3.1 Validación para la renovación rutinaria de certificados

Antes de renovar un certificado, la Autoridad de Certificación del CGCOM comprueba que la información empleada para verificar la identidad y los restantes datos del

suscriptor y de la persona física identificada en un certificado continúan siendo válidos.

Los métodos aceptables para dicha comprobación son los siguientes:

- El empleo del certificado vigente para su renovación, siempre que se trate de un certificado expedido por la AC-CGCOM y no se haya superado el plazo máximo legalmente establecido para esta posibilidad.

Si cualquier información del suscriptor o de la persona física identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.3.2 Validación para la renovación de certificados tras la revocación

Antes de generar un certificado a un suscriptor cuyo certificado fue revocado, la Autoridad de Certificación del CGCOM comprueba que la información empleada para verificar la identidad y los restantes datos del suscriptor y de la persona física identificada en el certificado continúan siendo válidos, en cuyo caso se aplicará lo dispuesto en la sección anterior

La renovación de certificados tras la revocación no será posible en los siguientes casos:

- El certificado fue revocado por emisión errónea a una persona diferente a la identificada en el certificado.
- El certificado fue revocado por emisión no autorizada por la persona física identificada en el certificado.
- El certificado revocado puede contener información errónea o falsa.

Si cualquier información del suscriptor o de la persona fisica identificada en el certificado ha cambiado, se registra adecuadamente la nueva información y se produce una autenticación completa, de acuerdo con lo establecido en la sección 3.2.

3.4 Identificación y autenticación de la solicitud de revocación

La Autoridad de Certificación del CGCOM autentica las peticiones e informes relativos a la revocación de un certificado, comprobando que provienen de una persona autorizada.

Los métodos aceptables para dicha comprobación son los siguientes:

- El envío de una solicitud de revocación por parte del suscriptor o de la persona física identificada en el certificado, por medio de la plataforma electrónica, de gestión del ciclo de vida de los certificados, o firmada electronicamente.
- La personación física en una oficina de un Colegio de Médicos o en una oficina del responsable de certificación de la organización del ámbito santiario.
- Otros medios de comunicación, como el teléfono, cuando existan garantías razonables de la identidad del solicitante de la revocación, a juicio de la Autoridad de Certificación del CGCOM.

4 Requisitos de operación del ciclo de vida de los certificados

4.1 Solicitud de emisión de certificado

4.1.1 Legitimación para solicitar la emisión

Antes de la emisión y entrega de un certificado, existe una solicitud de certificado, que puede producirse de oficio o a instancia de parte interesada.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por el Colegio profesional, o una Entidad del ámbito santiario .

4.1.2 Procedimiento de alta; Responsabilidades

Existen los siguientes tipos de solicitudes:

1) Solicitud electrónica de certificado de oficio (no contiene clave pública, ni se encuentra firmada digitalmente).
2) Solicitud electrónica de certificado de parte sin generación de claves (no contiene clave pública, ni se encuentra firmada digitalmente).

La Autoridad de Certificación del CGCOM recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Consejo General de Colegios Oficiales de Médicos , o por una Entidad del ámbito sanitario o a instancia de parte.

En el primer caso existe un documento, ya sea en soporte papel o en formato electrónico mediante la plataforma electrónica, referente a la solicitud de certificados, realizada por el Colegio o Entidad del ámbito sanitario a la Autoridad de Certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

A la solicitud se deberá acompañar documentación justificativa de la identidad y otras circunstancias de la persona física identificada en el certificado, de acuerdo con lo establecido en la sección 3.2.3.

Asimismo, el Colegio o la Entidad del ámbito sanitario acepta un convenio de suscriptor, en forma de condiciones generales de emisión.

4.2 Procesamiento de la solicitud de certificación

4.2.1 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de certificado, la Autoridad de Certificación del CGCOM se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

En caso afirmativo, la Autoridad de Certificación del CGCOM verifica la información proporcionada, verificando los aspectos descritos en la sección 3.2.

En caso de un certificado cualificado, la documentación justificativa de la aprobación de la solicitud ha de conservar debidamente registrada y con garantías de seguridad e integridad durante el plazo de 15 años desde la expiración del certificado o la finalización del servicio prestado, incluso todo en caso de pérdida anticipada de vigencia por revocación. Esta documentación podrá ser conservada de forma segura por medio de la plataforma electrónica.

El plazo de conservación de la documentación acreditativa de la solicitud de certificados no cualificados no podrá ser inferior a 5 años desde la expiración del certificado.

4.2.2 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la Autoridad de Certificación del CGCOM debe aprobar la solicitud del certificado y proceder a su emisión y entrega.

Si la verificación indica que la información no es correcta, o si se sospecha que no es correcta o que puede afectar a la reputación de la Autoridad de Certificación o de los suscriptores, la Autoridad de Certificación del CGCOM deniega la petición, o detiene su aprobación hasta haber realizado las comprobaciones complementarias que considere oportunas.

En caso que de las comprobaciones adicionales no se desprenda la corrección de las informaciones a verificar, se deniega la solicitud definitivamente.
La Autoridad de Certificación notifica al solicitante la aprobación o denegación de la solicitud.

CGCOM podrá automatizar los procedimientos de verificación de la corrección de la información que será contenida en los certificados, y de aprobación de las solicitudes, por medio de la plataforma electrónica.

4.2.3 Plazo para resolver la solicitud

La Autoridad de Certificación del CGCOM atiende las solicitudes de certificados por orden de llegada, en un plazo razonable, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.
Las solicitudes se mantienen activas hasta su aprobación o rechazo.

4.3 Emisión del certificado

4.3.1 Acciones de la Autoridad de Certificación del CGCOM durante el proceso de emisión

Tras la aprobación de la solicitud de certificación se procede a la emisión del certificado de forma segura y se pone a disposición del firmante para su aceptación, por medio de la plataforma electrónica y, cuando sea necesario, grabación en la tarjeta, de forma segura y se pone la misma a disposición del suscriptor el cual efectúa la entrega a la persona física identificada en el certificado para su aceptación, de acuerdo con lo establecido en la sección 4.3.2.

Los procedimientos establecidos en esta sección también se aplican en caso de renovación de certificados, dado que tal renovación implica la emisión de un nuevo certificado.

La Autoridad de Certificación del CGCOM:

- Protege la confidencialidad e integridad de los datos de registro de que dispone.
- Utiliza sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.
- Genera el par de claves, mediante un procedimiento de generación de certificados vinculado de forma segura con el procedimiento de generación de claves, y, cuando sea necesario, almacena la clave privada de forma segura y el correspondiente certificado en la tarjeta de la persona física identificada en el certificado.
- Emplea un procedimiento de generación de certificados que vincula de forma segura el certificado con la información de registro, incluyendo la clave pública certificada.
- Se asegura de que el certificado es emitido por sistemas que utilicen protección contra falsificación y que garanticen la confidencialidad de las claves durante el proceso de generación de dichas claves.
- Incluye en el certificado las informaciones establecidas en el Anexo I del Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, de acuerdo con lo establecido en las secciones 3.1.1 y 7.1
- Indica la fecha y la hora en que se expidió un certificado.
- Cuando se utilitza una tarjeta criptográfica, se emplea un procedimiento de gestión de dispositivos seguros de creación de firma que asegure que dicho dispositivo es entregado de forma segura al suscriptor.

4.3.2 Notificación de la emisión al suscriptor

La Autoridad de Certificación del CGCOM notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.4 Entrega y aceptación del certificado

4.4.1 Responsabilidades de la Autoridad de Certificación del CGCOM

La Autoridad de Certificación:

- Acredita definitivamente la identidad de la persona física identificada en el certificado, con la colaboración del Colegio o la Entidad del ámbito sanitario suscriptor, de acuerdo con lo establecido en las secciones 3.2.2 y 3.2.3.
- Entrega a la persona física identificada en el certificado. con la colaboración del Colegio, o la Entidad del ámbito sanitario suscriptor, cuando sea necesario, la tarjeta que contiene el certificado.
- Entrega a la persona física identificada en el certificado, con la colaboración del Colegio, o la Entidad del ámbito sanitario suscriptor, una hoja de entrega y aceptación del certificado, y cuando sea necesario también de la tarjeta, con los siguientes contenidos mínimos:

  a) Información básica acerca de la política y uso del certificado, incluyendo especialmente información acerca del prestador de servicios de certificación y de la Declaración de Prácticas de Certificación aplicable, como sus obligaciones, facultades y responsabilidades

  b) Información acerca del certificado y, cuando sea necesario, de la tarjeta.

  c) Reconocimiento por parte del poseedor, de recibir el certificado y cuando pertoque de la tarjeta, y la aceptación de los citados elementos.

  d) Obligaciones de la persona física identificada en el certificado.

  e) Responsabilidad de la persona física identificada en el certificado.

  f) Método de imputación exclusiva al poseedor de su clave privada y de sus datos de activación del certificado y, en su caso, del dispositivo criptográfico, de acuerdo con lo establecido en las secciones 6.2 y 6.4.

  g) La fecha del acto de entrega y aceptación.

- Obtener la firma, escrita o electrónica, de la persona identificada en el certificado. En la opción de la firma electrónica de la hoja de entrega, ésta se realiza por medio de los servicios de la plataforma electrónica.

El suscriptor colabora en estos procesos, debiendo registrar documentalmente los anteriores actos y remitir los citados documentos originales a la Autoridad de

Certificación del CGCOM. Cuando esta documentación se guarda electrónicamente se realiza por medio de los servicios de la plataforma electrónica.

Para ello, la Autoridad de Certificación del CGCOM remite al suscriptor el paquete de tarjetas solicitadas, junto con las hojas de entrega y aceptación correspondientes, y remite directamente a cada persona física identificada en el certificado. sus datos de activación de firma y otras informaciones.

Las tarjetas se entregan protegidas, de forma que únicamente la persona física identificada en el certificado puede hacer uso de las mismas.

4.4.2 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación ante el Colegio, la Entidad jurídica del ámbito sanitario suscriptor.

Cuando la persona física identificada en el certificado ha aceptado el certificado y, en su caso, la tarjeta, puede con los datos de activación recibidos y producir firmas electrónicas.

Una vez entregado o descargado el certificado, el usuario dispone de un periodo de 7 días para comprobar su correcto funcionamiento.

4.4.3 Publicación del certificado

La Autoridad de Certificación del CGCOM publica el certificado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes, siempre que se disponga de la autorización de la persona física identificada en el certificado.

4.4.4 Notificación de la emisión a terceros

La Autoridad de Certificación del CGCOM no realiza ninguna notificación de la emisión a terceras entidades.

4.5 Uso del par de claves y del certificado

4.5.1 Uso por el firmante

La Autoridad de Certificación del CGCOM obliga al firmante a:

- Facilitar a la AC-CGCOM información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4
- Cuando el certificado funcione conjuntamente con un DCCF, reconocer su capacidad de producción de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como otros tipos de firmas electrónicas y mecanismos de cifrado de información.
- Ser especialmente diligente en la custodia de su clave privada, con el fin de evitar usos no autorizados, de acuerdo con lo establecido en las secciones 6.1, 6.2 y 6.4
- Comunicar a la AC-CGCOM y a cualquier persona que se crea que pueda confiar en el certificado, sin retrasos injustificables:
    - La pérdida, el robo o el compromiso potencial de su clave privada.
    - La pérdida de control sobre su clave privada, debido al compromiso de los datos de activación (por ejemplo, el código PIN) o por cualquier otra causa.
    - Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
- Dejar de emplear la clave privada transcurrido el periodo indicado en la sección 6.3.2
- Dejar de emplear la clave privada en caso de compromiso de dicha clave, de revocación o de compromiso de las claves de la CA.

4.5.2 Responsabilidad civil del firmante

La AC-CGCOM obliga al firmante a responsabilizarse de:

- Que todas las informaciones suministradas por el firmante que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del certificado, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el firmante es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni título de prestador de servicios de certificación ni en ningún otro caso.

4.5.3 Uso por el suscriptor

4.5.3.1 Obligaciones del suscriptor del certificado

La Autoridad de Certificación del CGCOM obliga contractualmente al suscriptor a:

- Facilitar a la Autoridad de Certificación información completa y adecuada, conforme a los requisitos de esta Declaración de Prácticas de Certificación, en especial en lo relativo al procedimiento de registro.
- Manifestar su consentimiento previo a la emisión y entrega de un certificado.
- Emplear el certificado de acuerdo con lo establecido en la sección 1.4.
- Comunicar a la Autoridad de Certificación y a cualquier persona que el suscriptor crea que pueda confiar en el certificado, sin retrasos injustificables:
  a) Las inexactitudes o cambios en el contenido del certificado que conozca o pudiera conocer el suscriptor.
  b) La pérdida, la alteración, el uso no autorizado, el robo o el compromiso, cuando exista, de la tarjeta.
- Trasladar a las personas físicas identificadas en el certificado el cumplimiento de las obligaciones específicas de los mismos, y establecer mecanismos para garantizar el efectivo cumplimiento de las mismas.

- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Autoridad de Certificación del CGCOM, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación del prestador de servicios de certificación de la Autoridad de Certificación del CGCOM, sin permiso previo por escrito.

4.5.3.2 Responsabilidad civil del suscriptor de certificado

La Autoridad de Certificación del CGCOM obliga contractualmente al suscriptor a garantizar:

- Que todas las manifestaciones realizadas en la solicitud son correctas.
- Que todas las informaciones suministradas por el suscriptor que se encuentran contenidas en el certificado son correctas.
- Que el certificado se emplea exclusivamente para usos legales y autorizados, de acuerdo con la Declaración de Prácticas de Certificación.
- Que ninguna persona no autorizada ha tenido jamás acceso a la clave privada del suscriptor, y que es el único responsable de los daños causados por su incumplimiento del deber de proteger la clave privada.
- Que el suscriptor es una entidad final y no un prestador de servicios de certificación, y que no empleará la clave privada correspondiente a la clave pública listada en el certificado para firmar certificado alguno (o cualquier otro formato de clave pública certificada), ni Lista de Revocación de Certificados, ni a título de prestador de servicios de certificación ni en ningún otro caso.

4.5.4 Uso por el tercero que confía en certificados

4.5.4.1 Obligaciones del tercero que confía en certificados

La Autoridad de Certificación obliga contractualmente al tercero que confía en certificados a:

- Asesorarse de forma independiente acerca del hecho de que el certificado es apropiado para el uso que se pretende.
- Verificar la validez o revocación de los certificados emitidos, para lo que empleará información sobre el estado de los certificados.

- Verificar todos los certificados de la jerarquía de certificados, antes de confiar en la firma digital o en alguno de los certificados de la jerarquía, así como que la Entidad de Certificación emisora se encuentra en la Lista de Servicios de Confianza (TSL) emitida por el Organismo Acreditador Nacional.
- Reconocer que las firmas electrónicas verificadas, producidas en tarjeta o producidas en un dispositivo cualificado de creación de firma (DCCF) , tienen la consideración legal de firmas electrónicas cualificadas; esto es, equivalentes a firmas manuscritas, así como que el certificado permite la creación de otros tipos de firmas electrónicas y mecanismos de cifrado.
- Tener presente cualquier limitación en el uso del certificado, con independencia de que se encuentre en el propio certificado o en el contrato de tercero que confía en el certificado.
- Tener presente cualquier precaución establecida en un contrato o en otro instrumento, con independencia de su naturaleza jurídica.
- No monitorizar, manipular o realizar actos de ingeniería reversa sobre la implantación técnica de los servicios de certificación de la Autoridad de Certificación del CGCOM, sin permiso previo por escrito.
- No comprometer intencionadamente la seguridad de los servicios de certificación de la Autoridad de Certificación del CGCOM, sin permiso previo por escrito.

4.5.4.2 Responsabilidad civil del tercero que confía en certificados

La Autoridad de Certificación de CGCOM obliga contractualmente al suscriptor a manifestar:

- Que dispone de suficiente información para tomar una decisión informada con el objeto de confiar en el certificado o no.
- Que es el único responsable de confiar o no en la información contenida en el certificado.
- Que será el único responsable si incumple sus obligaciones como tercero que confía en el certificado.

4.6 Renovación de certificados

La renovación de los certificados exige la renovación de claves, por lo que debe atenderse a lo establecido en la sección 4.7.

4.7 Renovación de claves y certificados

4.7.1 Causas de renovación de claves y certificados

Los certificados vigentes se pueden renovar mediante un procedimiento específico y simplificado de solicitud, al efecto de mantener la continuidad del servicio de certificación. Cuando este procedimiento se realiza electrónicamente se utiliza exclusivamente la plataforma electrónica.

4.7.2 Legitimación para solicitar la renovación

Antes de la emisión y entrega de un certificado renovado, existe una solicitud de renovación de certificado, que puede producirse de oficio o a instancia de parte interesada.

Existe una autorización del suscriptor para que el solicitante pueda realizar la solicitud, que se instrumenta jurídicamente mediante una hoja de solicitud de certificados suscrita por el Colegio profesional .

4.7.3 Procedimientos de solicitud de renovación

4.7.3.1 Realización de la solicitud

La Autoridad de Certificación del CGCOM recibe solicitudes de certificados, realizadas de oficio por las entidades que integran la Consejo General de Colegios Oficiales de Médicos , o una Entidad jurídica del ámbito sanitario o a instancia de parte.

En el primer caso existe un documento, ya sea en soporte papel o en formato electrónico, referente a la solicitud de renovación de certificados, realizada por el Colegio, la Entidad jurídica del ámbito sanitario a la Autoridad de Certificación, el cual incluirá la indicación de la persona o personas a autorizar para realizar peticiones, así como, en su caso, los datos de las personas a las que se expedirán certificados.

La solicitud ha de indicar que los datos de los certificados no han cambiado, pudiendo únicamente indicar cambios en la dirección física, u otros datos, que permitan contactar a la persona física identificada en el certificado.

Asimismo, el Colegio o la Entidad jurídica del ámbito sanitario acepta un convenio de suscriptor, en forma de condiciones generales de emisión.
Cuando sea en formato electrónico, la solicitud se realiza exclusivamente por medio de la plataforma electrónica.

4.7.3.2 Ejecución de las funciones de identificación y autenticación

Una vez recibida una petición de renovación de certificado, la Entidad de Certificación de la CGCOM se asegura de que las solicitudes de certificado sean completas, precisas y estén debidamente autorizadas, antes de procesarlas.

4.7.3.3 Aprobación o rechazo de la solicitud

En caso de que los datos se verifiquen correctamente, la Autoridad de Certificación debe aprobar la solicitud de renovación del certificado y proceder a su emisión y entrega.

La Autoridad de Certificación notifica al solicitante la aprobación o denegación de la solicitud.

4.7.3.4 Plazo para resolver la solicitud

La Autoridad de Certificación del CGCOM atiende las solicitudes de renovación certificados por orden de llegada, en un plazo razonable anterior a la expiración de los certificados a revocar, pudiendo especificarse una garantía de plazo máximo en el convenio de emisión de certificados.
Las solicitudes de renovación se mantienen activas hasta su aprobación o rechazo.

4.7.4 Notificación de la emisión del certificado renovado

La Autoridad de Certificación del CGCOM notifica la emisión del certificado al suscriptor y a la persona física identificada en el certificado.

4.7.5 Conducta que constituye aceptación del certificado

La aceptación del certificado por la persona física identificada en el certificado se produce mediante la firma de la hoja de entrega y aceptación ante el suscriptor.

Cuando la persona física identificada en el certificado ha aceptado el certificado y, cuando sea necesario, la tarjeta, puede con los datos de activación recibidos producir firmas electrónicas.

Cuando la firma se produzca electrónicamente, ésta se realiza por medio de la plataforma electrónica.

4.7.6 Publicación del certificado

La Autoridad de Certificación del CGCOM publica el certificado renovado en el Depósito a que se refiere la sección 2.1, con los controles de seguridad pertinentes.

4.7.7 Notificación de la emisión a terceros

La Autoridad de Certificación del CGCOM no realiza ninguna notificación de la emisión a terceras entidades.

4.8 Modificación de certificados

La modificación de certificados, excepto la modificación de la clave pública certificada - que se considera renovación, será tratada como una nueva emisión de certificado, aplicándose lo descrito en las secciones 4.1, 4.2, 4.3 y 4.4.

4.9 Revocación de certificados

Esta sección detalla las prácticas relativas a la revocación de certificados.

4.9.1 Causas de revocación de certificados

La Autoridad de Certificación del CGCOM revoca un certificado cuando concurre alguna de las siguientes causas:
1) Circunstancias que afectan a la información contenida en el certificado:

a) Modificación de alguno de los datos contenidos en el certificado, después de la correspondiente emisión del certificado que incluye las modificaciones.

b) Descubrimiento de que alguno de los datos contenidos en la solicitud de certificado es incorrecto.

c) Descubrimiento de que alguno de los datos contenidos en el certificado es incorrecto.

2) Circunstancias que afectan a la seguridad de la clave o del certificado:

a) Compromiso de la clave privada o de la infraestructura o sistemas del prestador de servicios de certificación que emitió el certificado, siempre que afecte a la fiabilidad de los certificados emitidos a partir de ese incidente.

b) Infracción, por la Autoridad de Certificación del CGCOM, de los requisitos previstos en los procedimientos de gestión de certificados, establecidos en esta Declaración de Prácticas de Certificación.

c) Compromiso o sospecha de compromiso de la seguridad de la clave o del certificado emitido.

d) Acceso o utilización no autorizados, por un tercero, de la clave privada correspondiente a la clave pública contenida en el certificado.

e) El uso irregular del certificado por la persona física identificada en el certificado, o la falta de diligencia en la custodia de la clave privada.

3) Circunstancias que afectan a la seguridad de la tarjeta:

a) Compromiso o sospecha de compromiso de la seguridad de la tarjeta.

b) Pérdida o inutilización por daños de la tarjeta.

c) Acceso no autorizado, por un tercero, a los datos de activación de la persona física identificada en el certificado.

4) Circunstancias que afectan al suscriptor o a la persona física identificada en el certificado.:

a) Finalización de la relación jurídica de prestación de servicios entre la Autoridad de Certificación del CGCOM y el suscriptor.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado a la persona física identificada en el certificado..

c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción por el suscriptor o por la persona física identificada en el certificado, de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento de la persona física identificada en el certificado.

f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor a la persona física identificada en el certificado. o la finalización de la relación entre suscriptor y persona física identificada en el certificado..

g) Solicitud del suscriptor de revocación del certificado, de acuerdo con lo establecido en la sección 3.4.

5) Otras circunstancias:

a) La terminación del servicio de certificación de la CGCOM, de acuerdo con lo establecido en la sección 5.8.

b) El uso del certificado que sea dañino y continuado para la CGCOM o el proveedor técnico. En este caso, se considera que un uso es dañino en función de los siguientes criterios:

1º) La naturaleza y el número de quejas recibidas.

2º) La identidad de las entidades que presentan las quejas.

3º) La legislación relevante vigente en cada momento.

4º) La respuesta del suscriptor o de la persona física identificada en el certificado a las quejas recibidas.

4.9.2 Legitimación para solicitar la revocación

Pueden solicitar la revocación de un certificado:

- La propia persona identificada en el certificado.
- Un representante autorizado por el suscriptor.
- La Autoridad de Certificación del CGCOM, así como sus colaboradores en las tareas de registro y emisión.

4.9.3 Procedimientos de solicitud de revocación

La entidad que precise revocar un certificado debe solicitarlo a la Autoridad de Certificación del CGCOM o, en su caso, al Colegio, o el registrador que tramitó la solicitud de certificación, comprensiva de la siguiente información:

- Fecha de solicitud de la revocación.
- Identidad del suscriptor y del firmante.
- Razón detallada para la petición de revocación.
- Nombre y título de la persona que pide la revocación.
- Información de contacto de la persona que pide la revocación.

La solicitud debe ser autenticada, por su destinatario, de acuerdo con los requisitos establecidos en la sección 3.4 de esta política, antes de proceder a la revocación.

La AC-CGCOM podrá incluir cualquier otro requisito para la confirmación de las solicitudes de revocación[1].

El servicio de revocación se encuentra en la página de la Web de la AC-CGCOM en la siguiente dirección:

https://psc.cgcom.es/revocar_certificado

Tambien es posible realizar la solicitud de revocación por medio de la plataforma electrónica de gestión del ciclo de vida del certificado.

En caso de que el destinatario de una solicitud de revocación por parte de una persona física identificada en el certificado. fuera el Colegio, la Entidad jurídica del ámbito sanitario suscriptor, una vez autenticada la solicitud debe remitir una solicitud en este sentido a la Autoridad de Certificación del CGCOM.

La solicitud de revocación será procesada a su recepción.

Se informa al suscriptor y, en todo caso, a la persona física identificada en el certificado, acerca del cambio de estado del certificado revocado.

La Autoridad de Certificación del CGCOM no reactiva el certificado, una vez ha sido revocado.

[1] Ap 6.2.4-01 c) de ETSI EN 319 411-1

Tanto el servicio de gestión de las revocaciones como el servicio de consulta son considerados servicios críticos y así constan en el Plan de contingencias y el plan de continuidad de negocio de la AC CGCOM.

4.9.4 Plazo temporal de solicitud de revocación

Las solicitudes de revocación se remitirán de forma inmediata en cuanto se tenga conocimiento de la causa de revocación, y no será superior a las 24 horas[2].

4.9.5 Plazo temporal de procesamiento de la solicitud

La revocación se producirá inmediatamente cuando sea recibida, dentro del horario ordinario de operación de la Autoridad de Certificación del CGCOM.

4.9.6 Obligación de consulta de información de revocación de certificados

Los terceros deben comprobar el estado de aquellos certificados en los cuales desean confiar.

Un método por el cual se puede verificar el estado de los certificados es consultando la Lista de Revocación de Certificados más reciente emitida por la Autoridad de Certificación del CGCOM. El estado de la vigencia de los certificados también se puede comprobar por medio del protocolo OCSP.

Las Listas de Revocación de Certificados se publican en el Depósito de la Autoridad de Certificación del CGCOM, así como en las siguientes direcciones web, indicadas dentro de los certificados:

En la CGCOM QUALIFIED 2020
http://crl5.cgcom.es/crl/eccgcom.crl
http://crl6.cgcom.es/crl/eccgcom.crl

En la CGCOM QUALIFIED 2023
http://crl7.cgcom.es/crl/eccgcom.crl

[2] Ap 6.2.4.a) vi) de ETSI EN 319 411-1

http://crl8.cgcom.es/crl/eccgcom.crl

Otro método es la consulta de un servicio web que comunica los certificados revocados, según se indica posteriormente.

4.9.7 Frecuencia de emisión de listas de revocación de certificados (LRCs)

La Autoridad de Certificación del CGCOM emite una LRC al menos cada 24 horas.

La Autoridad de Certificación CGCOM y el provedor técnico emiten y publican **listas de revocados** de forma periódica siguiendo la siguiente tabla, e inmediatamente después de producirse una revocación.

CA	Frecuencia de emisión días	Duración
vinCAsign Qualified Authority	365 días	365 días
CGCOM	24 horas	48 horas

La LRC indica el momento programado de emisión de una nueva LRC, si bien, para reflejar revocaciones, se puede emitir una LRC antes del plazo indicado en la LRC anterior.
La LRC mantiene obligatoriamente el certificado revocado hasta que expira.

4.9.8 Plazo máximo de publicación de LRCs

Las LRCs se publican en el Depósito en un periodo inmediatamente razonable, tras su generación, que no supera unos pocos minutos en ningún caso.

4.9.9 Disponibilidad de servicios de comprobación en línea de estado de certificados

De forma alternativa, los terceros que confían en certificados podrán consultar el Depósito de certificados de la Autoridad de Certificación del CGCOM, que se encuentra disponible las 24 horas de los 7 días de la semana.

La dirección electrónica del Depósito es:

https://psc.gcom.es/deposito

Para comprobar la última CRL emitida en cada CA se debe descargar:

En la **CGCOM QUALIFIED 2020**
http://crl5.cgcom.es/crl/eccgcom.crl
http://crl6.cgcom.es/crl/eccgcom.crl

En la **CGCOM QUALIFIED 2023**
http://crl7.cgcom.es/crl/eccgcom.crl
http://crl8.cgcom.es/crl/eccgcom.crl

En caso de fallo de los sistemas de comprobación de estado de certificados por causas fuera del control de la Autoridad de Certificación del CGCOM, ésta deberá realizar sus mejores esfuerzos por asegurar que este servicio se mantenga inactivo el mínimo tiempo posible, que no podrá superar un día.

La Autoridad de Certificación del CGCOM suministra información a los terceros que confían en certificados acerca del funcionamiento del servicio de información de estado de certificados.

Los servicios de comprobación de estado de los certificados son de uso gratuito[3].

La AC-CGCOM mantiene disponible la información del estado de revocación pasado el período de validez del certificado[4], por medio del servicio OCSP. Esta disponibilidad

[3] CSS-6.3.10-01 de ETSI EN 319 411-2
[4] CSS-6.3.10-02 de ETSI EN 319 411-2

se mantiene en caso de finalización de los servicios PKI por parte de CGCOM, transfiriendo esta obligación a otro prestador.
En el supuesto que la CA emita la última CRL, el campo "nextUpdate" debera ser configurado[5] a "99991231235959Z", como se define en IETF RFC 5280[6]

4.9.10 Obligación de consulta de servicios de comprobación de estado de certificados

Resulta obligatorio consultar el estado de los certificados antes de confiar en los mismos.

El tercero que confía en el certificado que no emplee LRCs para comprobar la validez de un certificado, debe emplear el Depósito o el servicio web para ello.

4.9.11 Otras formas de información de revocación de certificados

La Autoridad de Certificación del CGCOM también informa acerca del estado de revocación de los certificados, mediante el protocolo OCSP, que permite conocer el estado de vigencia de los certificados en linea desde la dirección siguiente:
http://ocspservice.cgcom.es

4.9.12 Requisitos especiales en caso de compromiso de la clave privada

El compromiso de la clave privada de la Autoridad de Certificación del CGCOM es notificado, en la medida de lo posible, a todos los participantes en los servicios de certificación de la CGCOM, mediante la publicación de este hecho en la página web de la CGCOM, así como, si se considera necesario, en otros medios de comunicación, incluso en papel.

4.9.13 Solicitud de suspensión

Esta entidad no realiza suspensión de certificados

[5] REV-6.3.9-01 de la ETSI EN 319 411-2 -> CSS-6.3.9-06 de la ETSI EN 319 411-1
[6] Ap 4.1.2.5 (validity) de la IETF RFC 5280

4.9.14 Procedimientos para la petición de suspensión

Esta entidad no realiza suspensión de certificados

4.9.15 Período máximo de suspensión

Esta entidad no realiza suspensión de certificados

4.10 Servicios de comprobación de estado de certificados

4.10.1 Características operativas de los servicios

Los servicios de comprobación de estado de certificados se prestan mediante una interfaz de consulta web, a través del Depósito de los certificados, y mediante un servicio web específico de consulta.

4.10.2 Disponibilidad de los servicios

Los servicios de comprobación de estado de certificados se encuentran disponibles las 24 horas del día, los 7 días de la semana, durante todo el año, con excepción de las paradas programadas.

4.10.3 Características opcionales

Los servicios de comprobación de estado de certificados no presentan características opcionales.

4.11 Finalización de la suscripción

Transcurrido el periodo de vigencia del certificado, finalizará la suscripción al servicio.

Como excepción, el suscriptor puede mantener el servicio vigente, solicitando la renovación del certificado, con la antelación que determina esta Declaración de Prácticas de Certificación.

La Autoridad de Certificación del CGCOM puede emitir de oficio un nuevo certificado, mientras los suscriptores mantengan dicho estado.

4.12 Depósito y recuperación de claves

4.12.1 Política y prácticas de depósito y recuperación de claves

La Autoridad de Certificación del CGCOM no presta servicios de depósito y recuperación de claves.

4.12.2 Política y prácticas de encapsulado y recuperación de claves de sesión

Sin estipulación.

5 Controles de seguridad física, de gestión y de operaciones

En este apartado diferenciaremos dominios de actuación de la Autoridad de Certificación del Consejo General de Colegios Oficiales de Médicos .

De esta forma podemos encontrar:

Dominio de creación de certificados.
Los controles de seguridad física, de gestión y de operaciones en el dominio de creación de los certificados son operados por el proveedor técnico.

El proveedor técnico está sujeto a las validaciones anuales de la norma ISO/IEC 27001 que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna
Los controles de seguridad física, de gestión y de operaciones en el dominio del registro de los usuarios y, cuando sea necesario, la gestión de tarjetas criptográficas son operados por una entidad u organización perteneciente a la CGCOM (por ejemplo un Colegio de Médicos), o una Entidad del ámbito sanitario.

5.1 Controles de seguridad física

La Autoridad de Certificación del CGCOM, por medio de su proveedor técnico, ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de generación técnica de los certificados.

Las instalaciones del proveedor técnico cuentan con sistemas de mantenimiento preventivo y correctivo con asistencia 24h-365 días al año con asistencia en las 24 horas siguientes al aviso.

La Autoridad de Certificación de CGCOM, en las instalaciones de una entidad interna, ha establecido controles de seguridad física y ambiental para proteger los recursos de las instalaciones donde se encuentran los sistemas, los propios sistemas y los equipamientos empleados para las operaciones de registro y aprobación de las solicitudes de certificados, así como de la gestión de las tarjetas criptográficas de médicos colegiados.

En concreto, la política de seguridad física y ambiental aplicable a los servicios de registro y aprobación de las solicitudes de certificados, así como de la gestión, cuando sea necesario, de las tarjetas criptográficas, ha establecido prescripciones para las siguientes contingencias:

- Controles de acceso físico.
- Protección antirrobos.
- Allanamiento y entrada no autorizada.
- Salida no autorizada de equipamientos, informaciones, soportes y aplicaciones relativos a componentes empleados para los servicios del prestador de servicios de certificación.

Estas medidas resultan aplicables a las instalaciones de la entidad interna donde se realiza la aprobación de las solicitudes de certificados y, cuando sea necesario, la gestión de las tarjetas criptográficas bajo la plena responsabilidad de la Autoridad de Certificación del CGCOM.

La Autoridad de Certificación del CGCOM, en las instalaciones de la entidad interna, ha establecido medidas de seguridad y de protección de datos personales suficientes en relación con los servicios de aprobación y de generación técnica y de manipulado de tarjetas.

5.1.1 Localización y construcción de las instalaciones

Dominio de creación de certificados

La protección física se logra mediante la creación de perímetros de seguridad claramente definidos en torno a los servicios. La calidad y solidez de los materiales de construcción de las instalaciones garantiza unos adecuados niveles de protección frente a intrusiones por la fuerza bruta, ubicándose, además, en una zona de bajo riesgo de desastres y permitiendo un rápido acceso.
La sala donde se realizan las operaciones criptográficas en el Centro de Procesamiento de Datos:

- Cuenta con redundancia en sus infraestructuras.
- Cuenta con varias fuentes alternativas de electricidad y refrigeración en caso de emergencia.
- Las operaciones de mantenimiento no requieren que el Centro esté offline en ningún momento.
- Cuenta con una disponibilidad del 99,982 %

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.La Autoridad de Certificación del CGCOM, en las instalaciones de la entidad interna dispone de instalaciones que protegen físicamente la prestación de los servicios de aprobación de solicitudes de certificados, de gestión –cuando sea necesario- de tarjetas y de gestión de revocación, del compromiso causado por acceso no autorizado a los sistemas o a los datos, así como a la divulgación de los mismos.

5.1.2 Acceso físico

Dominio de creación de certificados
CGCOM, en las instalaciones de su proveedor técnico, dispone de tres niveles de seguridad física (Entrada del Edificio donde se ubica el CPD, acceso a la sala del CPD y acceso al rack) para la protección del servicio de generación de certificados, debiendo accederse desde los niveles inferiores a los niveles superiores.

El acceso físico a las dependencias del proveedor técnico donde se llevan a cabo procesos de certificación está limitado y protegido mediante una combinación de medidas físicas y procedimentales. Así:

- Está limitado a personal expresamente autorizado, con identificación en el momento del acceso y registro del mismo, incluyendo filmación por circuito cerrado de televisión y su archivo.
- El acceso a las salas se realiza con lectores de tarjeta de identificación y es gestionado por un sistema informático que mantiene un log de entradas y salidas automático.
- Para el acceso al rack donde se ubican los procesos criptográficos es necesario la autorización previa del proveedor técnico a los administradores del servicio de hospedaje que disponen de la llave para abrir la jaula.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna

La Autoridad de Certificación del CGCOM, en las instalaciones de la entidad interna, dispone de la adecuada y suficiente seguridad física para la protección del servicio de aprobación de las solicitudes de certificados y de gestión, cuando sea necesario, de las tarjetas criptográficas.

5.1.3 Electricidad y aire acondicionado

Dominio de creación de certificados

CGCOM, en las instalaciones del proveedor técnico, dispone de equipos estabilizadores de corriente y un sistema de alimentación eléctrica de equipos duplicado con un grupo electrógeno.

Las salas que albergan equipos informáticos cuentan con sistemas de control de temperatura con equipos de aire acondicionado.

5.1.4 Exposición al agua

Dominio de creación de certificados

La Autoridad de Certificación del CGCOM, en las instalaciones del proveedor técnico, están ubicadas en una zona de bajo riesgo de inundación.
Las salas donde se albergan equipos informáticos disponen de un sistema de detección de humedad.

5.1.5 Prevención y protección de incendios

Dominio de creación de certificados
Todas las instalaciones y activos de la Autoridad de Certificación del CGCOM, en las instalaciones del proveedor técnico, cuentan con sistemas automáticos de detección y extinción de incendios.

Dominio de registro de usuarios y gestión, cuando sea necesario, de tarjetas por entidad interna
Todas las instalaciones y activos de la Autoridad de Certificación del CGCOM, en las instalaciones de las entidades internas, cuentan con sistemas de extinción de incendios, de acuerdo con las normativas locales de prevención de incendios.

5.1.6 Almacenamiento de soportes

Dominio de creación de certificados

Únicamente el personal autorizado tiene acceso a los medios de almacenamiento.
La información de más alto nivel de clasificación se guarda en una caja de seguridad fuera de las instalaciones del Centro de Procesamiento de Datos.

5.1.7 Tratamiento de residuos

Dominio de creación de certificados

La eliminación de soportes, tanto en formato papel como magnéticos, se realizan mediante mecanismos que garanticen la imposibilidad de recuperación de la información.
En el caso de soportes magnéticos, se procede al formateo, borrado permanente, o destrucción física del soporte, mediante software especializado que realice un mínimo de 3 pasadas de borrado y con patrones de borrado variable.
En el caso de documentación en papel, mediante trituradoras o en papeleras dispuestas al efecto para posteriormente ser destruidos, bajo control.

5.1.8 Copia de respaldo fuera de las instalaciones

Dominio de creación de certificados

La AC CGCOM utiliza un almacén externo seguro para la custodia de documentos, dispositivos magnéticos y electrónicos que son independientes del centro operacional.

Se requieren al menos dos personas autorizadas expresamente para el acceso, depósito o retirada de dispositivos.

5.2 Controles de procedimientos

Dominio de creación de certificados

La Autoridad de Certificación del CGCOM garantiza que sus sistemas se operan de forma segura, para lo cual ha establecido e implantado procedimientos para las funciones que afectan a la provisión de sus servicios.

El personal al servicio de la Autoridad de Certificación del CGCOM ejecuta los procedimientos administrativos y de gestión de acuerdo con la política de seguridad.

5.2.1 Funciones fiables

Dominio de creación de certificados

La Autoridad de Certificación de la CGCOM, en las instalaciones del proveedor técnico, ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- **Auditor Interno**: Responsable del cumplimiento de los procedimientos operativos. Se trata de una persona externa al departamento de Sistemas de Información. Las tareas de Auditor interno son incompatibles en el tiempo con las tareas de Certificación e incompatibles con Sistemas. Estas funciones estarán subordinadas a la jefatura de operaciones, reportando tanto a ésta como a la dirección técnica.
- **Administrador de Sistemas**: Responsable del funcionamiento correcto del hardware y software soporte de la plataforma de certificación
- **Administrador de CA**: Responsable de las acciones a ejecutar con el material criptográfico, o con la realización de alguna función que implique la activación de las claves privadas de las autoridades de certificación descritas en este documento, o de cualquiera de sus elementos.
- **Operador de CA**: Responsable necesario conjuntamente con el Administrador de CA de la custodia de material de activación de las claves criptográficas, también responsable de las operaciones de backup y mantenimiento de la AC.
- **Administrador de RA**: Persona responsable de aprobar las peticiones de certificación realizadas por el suscriptor. .
- **Operador de revocación**: Persona responsable de realizar revocaciones de las peticiones de certificación realizadas por el suscriptor..
- **Responsable de Seguridad**: Encargado de coordinar, controlar y hacer cumplir las medidas de seguridad definidas por las políticas de seguridad del proveedor técnico. Debe encargarse de los aspectos relacionados con la seguridad de la información: lógica, física, redes, organizativa, etc.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos. Estas personas realizarán sus funciones basándose en el principio de menor privilegio.

Dominio de registro de usuarios y gestión, cuando sea necesario, de tarjetas por entidad interna

La Autoridad de Certificación de CGCOM, por medio de la entidad interna, ha identificado, de acuerdo con su política de seguridad, las siguientes funciones o roles con la condición de fiables:

- Personal de atención al cliente.
- Personal responsable de la seguridad.
- Administradores del sistema.
- Operadores del sistema.

Las personas que ocupan los puestos anteriores se encuentran sometidas a procedimientos de investigación y control específicos.

5.2.2 Número de personas por tarea

Dominio de creación de certificados

El proveedor técnico garantiza al menos dos personas para realizar las tareas que se detallen en las Políticas de Certificación correspondientes. Especialmente en la manipulación del dispositivo de custodia de las claves de la Autoridad de Certificación raíz e intermedias.

5.2.3 Identificación y autenticación para cada función

Dominio de creación de certificados

Las personas asignadas para cada rol son identificadas por el auditor interno que se asegurara que cada persona realiza las operaciones para las que está asignado.
Cada persona solo controla los activos necesarios para su rol, asegurando así que ninguna persona accede a recursos no asignados.
El acceso a recursos se realiza dependiendo del activo mediante tarjetas criptográficas y códigos de activación.

5.2.4 Roles que requieren separación de tareas

Las siguientes tareas son realizadas, al menos, por dos personas:
- Emisión y revocación de certificados, y acceso al depósito.

- Generación, emisión y destrucción de certificados de la Entidad de Certificación.
- Puesta en producción de la Entidad de Certificación.

5.2.5 Arranque y parada del sistema de gestión PKI

El sistema de PKI se compone de los siguientes módulos:
- Componente/módulo de gestión de la Autoridad de Certificación Subordinada
- Componente/módulo de gestión de la Autoridad de Registro
- Componente/módulo de gestión de solicitudes
- Componente/módulo de gestión de claves (HSM)
- Componente/módulo de bases de datos
- Componente/módulo de gestión de CRL
- Componente/módulo de gestión del servicio de OCSP

5.3 Controles de personal

5.3.1 Requisitos de historial, calificaciones, experiencia y autorización

Dominio de creación de certificados

Todo el personal que realiza tareas calificadas como confiables, lleva al menos **un año** trabajando en el centro de producción y tiene contratos laborales fijos.
Todo el personal está cualificado y ha sido instruido convenientemente para realizar las operaciones que le han sido asignadas.
El personal en puestos de confianza se encontrará libre de intereses personales que entran en conflicto con el desarrollo de la función que tenga encomendada.

Dominio de registro

La AC CGCOM se asegura de que el personal de registro o Administradores de AR es confiable y pertenece a los Colegios Oficiales de Médicos o del organismo delegado para realizar las tareas de registro.

El Administrador de AR habrá realizado un curso de preparación para la realización de las tareas de validación de las peticiones.
En general, la AC CGCOM retirará de sus funciones de confianza a un empleado cuando se tenga conocimiento de la existencia de la comisión de algún hecho delictivo que pudiera afectar al desempeño de sus funciones.
La AC CGCOM no asignará a un sitio confiable o de gestión a una persona que no sea idónea para el puesto, especialmente por haber sido condenada por delito o falta que afecte su idoneidad para el puesto. Por este motivo, previamente se realiza una investigación, hasta donde permita la legislación aplicable, relativa a los siguientes aspectos:

- Estudios, incluyendo titulación alegada.
- Trabajos anteriores, hasta cinco años, incluyendo referencias profesionales y comprobación que realmente se realizó el trabajo alegado.
- Morosidad

5.3.2 Procedimientos de investigación de historial

La Autoridad de Certificación del CGCOM, antes de contratar a una persona o de que ésta acceda al puesto de trabajo, realiza las siguientes comprobaciones:

- Referencias de los trabajos de los últimos años
- Referencias profesionales
- Estudios, incluyendo titulación alegada.

La AC-CGCOM realiza dichas comprobaciones con observancia estricta del 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 la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

La investigación se repetirá con una periodicidad suficiente.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente aplicable.

Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.

- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

La AC-CGCOM realiza dichas comprobaciones con observancia estricta del Reglamento general de protección de datos.

Todas las comprobaciones se realizan hasta donde lo permite la legislación vigente en cada momento y lugar. Los motivos que pueden dar lugar a rechazar al candidato a un puesto fiable son los siguientes:

- Falsedades en la solicitud de trabajo, realizadas por el candidato.
- Referencias profesionales muy negativas o muy poco fiables en relación con el candidato.

En la solicitud para el puesto de trabajo se informa acerca de la necesidad de someterse a una investigación previa, advirtiéndose de que la negativa a someterse a la investigación implicará el rechazo de la solicitud.

5.3.3 Requisitos de formación

Dominio de creación de certificados

El proveedor técnico forma al personal en puestos fiables y de gestión, hasta que alcanzan la cualificación necesaria, manteniendo archivo de dicha formación.
Los programas de formación son actualizados y mejorados de forma periódica.
La formación incluye, al menos, los siguientes contenidos:

- Principios y mecanismos de seguridad de la jerarquía de certificación, así como el entorno de usuario de la persona a formar.
- Tareas que debe realizar la persona.
- Políticas y procedimientos de seguridad del proveedor técnico. Uso y operación de maquinaria y aplicaciones instaladas.
- Gestión y tramitación de incidentes y compromisos de seguridad.
- Procedimientos de continuidad de negocio y emergencia.
- Procedimiento de gestión y de seguridad en relación con el tratamiento de los datos de carácter personal.

5.3.4 Requisitos y frecuencia de actualización formativa

Dominio de creación de certificados

El proveedor técnico, actualiza la formación del personal de acuerdo con sus necesidades, y con la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación

Dominio de Registro

La Autoridad de Certificación del CGCOM, actualiza la formación del personal de acuerdo con las necesidades y la frecuencia suficientes para cumplir sus funciones de forma competente y satisfactoria, especialmente cuando se realicen modificaciones sustanciales en las tareas de certificación, de acuerdo con su plan de formación.

5.3.5 Secuencia y frecuencia de rotación laboral

No aplicable.

5.3.6 Sanciones para acciones no autorizadas

La Autoridad de Certificación del CGCOM y el proveedor técnico disponen de un sistema sancionador, para depurar las responsabilidades derivadas de acciones no autorizadas, adecuado a la legislación laboral aplicable y, en especial, coordinado con el sistema sancionador del convenio colectivo que resulte de aplicación al personal.

Las acciones disciplinarias incluyen la suspensión y el despido de la persona responsable de la acción dañina, de forma proporcionada a la gravedad de la acción no autorizada.

5.3.7 Requisitos de contratación de profesionales

Los empleados contratados para realizar tareas confiables firman con anterioridad las cláusulas de confidencialidad y los requerimientos operacionales empleados por el proveedor técnico. Cualquier acción que comprometa la seguridad de los procesos aceptados podrían, una vez evaluados, dar lugar al cese del contrato laboral.

En el caso de que todos o parte de los servicios de certificación sean operados por un tercero, los controles y previsiones realizadas en esta sección, o en otras partes de la DPC, serán aplicados y cumplidos por el tercero que realice las funciones de operación de los servicios de certificación, no obstante lo cual, la entidad de certificación será responsable en todo caso de la efectiva ejecución. Estos aspectos quedan concretados en el instrumento jurídico utilizado para acordar la prestación de los servicios de certificación por un tercero distinto a CGCOM o el proveedor técnico.

5.3.8 Suministro de documentación al personal

El prestador de servicios de certificación suministrará la documentación que estrictamente precise su personal en cada momento, al objeto de realizar su trabajo de forma competente y satisfactoria.

5.4 Procedimientos de auditoria de seguridad

Dominio de creación de certificados

El proveedor técnico está sujeto a las validaciones anuales de la norma ISO/IEC 27001, que regula el establecimiento de procesos adecuados para garantizar una correcta gestión de la seguridad en los sistemas de información que dan soporte a los procesos de certificación electrónica.

Dominio de registro

La Autoridad de Certificación Consejo General de Colegios Oficiales de Médicos del Consejo General de Colegios Oficiales de Médicos realiza las oportunas evaluaciones de conformidad para la adecuación al Reglamento (UE) 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, y de las normas ETSI EN 319 401, ETSI EN 319 411-1 y ETSI EN 319 411-2.

La Autoridad de Certificación Consejo General de Colegios Oficiales de Médicos del Consejo General de Colegios Oficiales de Médicos está sujeta a las medidas de seguridad que correspondan de conformidad con la normativa de aplicación en materia de protección de datos.

5.4.1 Tipos de eventos registrados y su frecuencia

Dominio de creación de certificados

El proveedor técnico produce y guarda registro, al menos, de los siguientes eventos relacionados con la seguridad de la entidad:

- Encendido y apagado del sistema.
- Intentos de creación, borrado, establecimiento de contraseñas o cambio de privilegios.
- Intentos de inicio y fin de sesión.
- Intentos de accesos no autorizados al sistema de la AC a través de la red.
- Intentos de accesos no autorizados al sistema de archivos.
- Acceso físico a los logs.
- Cambios en la configuración y mantenimiento del sistema.
- Registros de las aplicaciones de la AC.
- Encendido y apagado de la aplicación de la AC.
- Cambios en los detalles de la AC y/o sus claves.
- Cambios en la creación de políticas de certificados.
- Generación de claves propias.

- Creación y revocación de certificados.
- Registros de la destrucción de los medios que contienen las claves y los datos de activación.
- Eventos relacionados con el ciclo de vida del módulo criptográfico, como la recepción, el uso y la desinstalación del mismo.
- Las actividades de los cortafuegos y enrutadores.
- La ceremonia de generación de claves y las bases de datos de gestión de claves.
- Registros de acceso físico.
- Mantenimientos y cambios de configuración del sistema.
- Cambios en el personal.
- Informes de compromisos y discrepancias.
- Registros de la destrucción de material que contenga información de claves, datos de activación o información personal del suscriptor, en caso de certificados individuales, o de la persona física identificada en el certificado, en caso de certificados de organización.
- Posesión de datos de activación, para operaciones con la clave privada de la Entidad de Certificación.
- Informes completos de los intentos de intrusión física en las infraestructuras que dan soporte a la emisión y gestión de certificados. Las entradas del registro incluyen los siguientes elementos:
- Fecha y hora de la entrada.
- Número de serie o secuencia de la entrada, en los registros automáticos.
- Identidad de la entidad que entra el registro.
- Tipo de entrada.

Dominio de gestión de tarjetas por entidad interna.

Quedan registrados todos los sucesos relacionados con la preparación de los dispositivos cualificados de creación de firmas (DCCF, o en inglés QSCD) que son usados por los firmantes o custodios.

5.4.2 Frecuencia de tratamiento de registros de auditoría

El proveedor técnico revisa sus logs cuando se produce una alerta del sistema motivada por la existencia de algún incidente.
El procesamiento de los registros de auditoría consiste en una revisión de los registros que incluye la verificación de que éstos no han sido manipulados, una breve inspección de todas las entradas de registro y una investigación más profunda de cualquier alerta o irregularidad en los registros. Las acciones realizadas a partir de la revisión de auditoría están documentadas.
El proveedor técnico mantiene un sistema que permite garantizar:
- Espacio suficiente para el almacenamiento de logs
- Que los ficheros de logs no se reescriben.
- Que la información que se guarda incluye como mínimo: tipo de evento, fecha y hora, usuario que ejecuta el evento y resultado de la operación.
- Los ficheros de logs se guardarán en ficheros estructurados susceptibles de incorporar en una BBDD para su posterior exploración.

5.4.3 Periodo de conservación de registros de auditoría

Dominio de creación de certificados
La AC CGCOM, junto con el proveedor técnico almacena la información de los logs al menos durante 15 años.

5.4.4 Protección de los registros de auditoría

Dominio de creación de certificados
Los logs de los sistemas:
- Están protegidos frente a posibles manipulaciones, borrados o eliminaciones mediante la firma de los ficheros que los contienen.
- Son almacenados en dispositivos ignífugos.
- Se protege su disponibilidad mediante el almacén en instalaciones externas al centro donde se ubica la AC.
El acceso a los ficheros de logs está reservado solo a las personas autorizadas. Asimismo, los dispositivos son manejados en todo momento por personal autorizado. Existe un procedimiento interno donde se detallan los procesos de gestión de los dispositivos que contienen datos de logs de auditoría.

5.4.5 Procedimientos de copia de respaldo

Dominio de creación de certificados

El proveedor técnico dispone de un procedimiento adecuado de copias de seguridad de manera que, en caso de pérdida o destrucción de archivos relevantes, estén disponibles en un periodo corto de tiempo las correspondientes copias de seguridad de los logs.
El proveedor técnico tiene implementado un procedimiento de copias de seguridad seguro de los logs de auditoría, realizando semanalmente una copia de todos los logs en un medio externo. Adicionalmente se mantiene copia en centro de custodia externo.

5.4.6 Localización del sistema de acumulación de registros de auditoría

Dominio de creación de certificados
La información de la auditoria de eventos es recogida internamente y de forma automatizada por el sistema operativo, las comunicaciones de red y el software de gestión de certificados, además de por los datos manualmente generados, que serán almacenados por el personal debidamente autorizado. Todo ello compone el sistema de acumulación de registros de auditoría.

5.4.7 Notificación del evento de auditoria al causante del evento

Dominio de creación de certificados
Cuando el sistema de acumulación de registros de auditoría registre un evento, no es preciso enviar una notificación al individuo, organización, dispositivo o aplicación que ha causado dicho evento.

5.4.8 Análisis de vulnerabilidades

Dominio de creación de certificados
El análisis de vulnerabilidades queda cubierto por los procesos de auditoría del proveedor técnico. Los análisis de vulnerabilidades deben ser ejecutados, repasados y revisados por medio de un examen de estos acontecimientos monitorizados. Estos análisis son ejecutados trimestralmente.

Los datos de auditoría de los sistemas son almacenados con el fin de ser utilizados en la investigación de cualquier incidencia y localizar vulnerabilidades.

Dominio de registro
Las vulnerabilidades detectadas se tratarán según los procedimientos existentes, los cuales incluyen clasificación, categorización, identificación y aplicación de parches. Serán priorizadas en función de su criticidad, estableciéndose un plazo máximo de resolución de 48 horas paras las categorizadas como críticas.

5.5 Archivo de informaciones

Para todos los dominios
La Autoridad de Certificación del CGCOM, garantiza que toda la información relativa a los certificados se guarda durante un período de tiempo apropiado, según lo establecido en la sección 5.5.2 de esta política.

5.5.1 Tipos de registros archivados

Dominio de creación de certificados
Los siguientes documentos implicados en el ciclo de vida del certificado son almacenados por el proveedor técnico (o por las entidades de registro):

- Todos los datos de auditoría de sistema (PKI, TSA y OCSP).
- Todos los datos relativos a los certificados, incluyendo los contratos con los firmantes y los datos relativos a su identificación y ubicación
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al proceso de revocación.
- Todas aquellas elecciones específicas que el firmante o el subscriptor disponga durante el acuerdo de subscripción.
- Tipo de documento presentado en la solicitud del certificado.
- Identidad de la Entidad de Registro que acepta la solicitud de certificado.
- Número de identificación único proporcionado por el documento anterior.
- Todos los certificados emitidos o publicados.
- CRLs emitidas o registros del estado de los certificados generados.

- Historial de claves generadas.
- Comunicaciones entre los elementos de la PKI.
- Políticas y Prácticas de Certificación
- Todos los datos de auditoría identificados en la sección 5.4
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.

El proveedor técnico es responsable del correcto archivo de todo este material.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

La Autoridad de Certificación del CGCOM, en las instalaciones de la subcontratada o de la entidad interna, archiva:

- Todos los datos de auditoría identificados en la sección 5.4.
- Información de solicitudes de certificación.
- Documentación aportada para justificar las solicitudes de certificación.
- Información del ciclo de vida del certificado.
- Solicitudes de emisión y revocación de certificados, incluidos todos los informes relativos al poceso de revocación[7].
- Todas aquellas elecciones específicas que el firmante o el subscriptor disponga durante el acuerdo de subscripción[8].

5.5.2 Periodo de conservación de registros

Para todos los dominios

La Autoridad de Certificación del CGCOM archiva los registros especificados anteriormente durante 15 años.

.

[7] REV-6.4.5-09 de ETSI EN 319 411-1

[8] REG-6.4.5-04 d) de ETSI EN 319 411-1

5.5.3 Protección del archivo

Para todos los dominios

La Autoridad de Certificación de CGCOM protege el archivo de forma que sólo personas fiables debidamente autorizadas puedan obtener acceso al mismo. El archivo es protegido contra visualización, modificación, borrado o cualquier otra manipulación mediante su almacenamiento en un sistema fiable.

El proveedor técnico asegura la correcta protección de los archivos mediante la asignación de personal cualificado para su tratamiento y el almacenamiento en cajas de seguridad ignífugas e instalaciones externas.

5.5.4 Procedimientos de copia de respaldo

Dominio de creación de certificados

El proveedor técnico dispone de un centro de almacenamiento externo para garantizar la disponibilidad de las copias del archivo de ficheros electrónicos. Los documentos físicos se encuentran almacenados en lugares seguros de acceso restringido solo a personal autorizado.

El proveedor técnico como mínimo realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos y realiza copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, el proveedor técnico (o las organizaciones que realizan la función de registro) guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Entidad de certificación.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

La Autoridad de Certificación del CGCOM, en las acciones realizadas por la subcontratada o por la entidad interna, realiza copias de respaldo incrementales diarias de todos sus documentos electrónicos, y copias de respaldo completas semanalmente para casos de recuperación de datos.

Además, la Autoridad de Certificación, en la entidad interna, guarda copia de los documentos en papel en un lugar seguro diferente de las instalaciones de la propia Autoridad de Certificación.

5.5.5 Requisitos de sellado de fecha y hora

La hora empleada para registrar los sucesos del registro de auditoría deberá ser sincronizada con la UTC, como mínimo, una vez al día[9].

No es necesario que esta información se encuentre firmada digitalmente.

Dominio de creación de certificados
Los registros están fechados con una fuente fiable vía NTP desde su propio CPD, con un Stratum 1

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
Las bases de datos de la Autoridad de Certificación emplean registros fiables de fecha y hora.

5.5.6 Localización del sistema de archivo

Dominio de creación de certificados
La AC CGCOM dispone de un sistema centralizado de recogida de información de la actividad de los equipos implicados en el servicio de gestión de certificados.

5.5.7 Procedimientos de obtención y verificación de información de archivo

Dominio de creación de certificados
La AC CGCOM dispone de un documento de seguridad informática donde se describe el proceso para verificar que la información archivada es correcta y accesible.

[9] REQ-7.10-06 de la ETSI EN 319 401

5.6 Renovación de claves

Dominio de creación de certificados

Con anterioridad a que el uso de la clave privada de la AC caduque, se realizará un cambio de claves. La antigua AC y su clave privada solo se usarán para la firma de CRLs mientras existan certificados activos emitidos por dicha AC. Se generará una nueva AC con una clave privada nueva y un nuevo DN.
El cambio de claves del suscriptor es materializado mediante la realización de un nuevo proceso de emisión.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
No aplicable

5.7 Compromiso de claves y recuperación de desastre

5.7.1 Procedimientos de gestión de incidencias y compromisos

Dominio de creación de certificados
Son almacenadas copias de seguridad de la siguiente información en instalaciones de almacenamiento externo al proveedor técnico, que se ponen a disposición en caso de compromiso o desastre: datos técnicos de solicitud de certificados, datos de auditoría y registros de la base de datos de todos los certificados emitidos.
Las copias de seguridad de las claves privadas del proveedor técnico son generadas y mantenidas de acuerdo con lo establecido en la sección 5.2.4, del presente documento.

Dominio de registro de usuarios y gestión de tarjetas por entidad interna.
Se guardan copias de seguridad de la siguiente información de la Autoridad de Certificación, en instalaciones de almacenamiento externo a la Autoridad de Certificación, que se ponen a disposición en caso de compromiso o desastre: datos de solicitud de certificados.

5.7.2 Corrupción de recursos, aplicaciones o datos

Dominio de creación de certificados

Cuando acontezca un evento de corrupción de recursos, aplicaciones o datos, se comunicará la incidencia a seguridad, y se iniciarán los procedimientos de gestión oportunos, que contemplan el escalado y la investigación y respuesta al incidente. Si resulta necesario, se iniciarán los procedimientos de compromiso de claves o de recuperación de desastres del proveedor técnico. Compromiso de la clave privada de la entidad

En caso de compromiso de la clave privada de la entidad puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos[10].

Dominio de creación de certificados

En caso de sospecha o conocimiento del compromiso del proveedor técnico, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación y desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada del proveedor técnicopuede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos.

El proveedor técnico ha desarrollado un Plan de contingencias para recuperar los sistemas críticos, si fuera necesario en un centro de datos alternativo.

El caso de compromiso de la clave raíz debe tomarse como un caso separado en el proceso de contingencia y continuidad de negocio. Esta incidencia afecta, en caso de sustitución de las claves, a los reconocimientos por diferentes aplicativos y servicios privados y públicos. Una recuperación de la efectividad de las claves en términos de negocio dependerá principalmente de la duración de estos procesos. El documento de contingencia y continuidad de negocio tratará los términos puramente operativos para que las nuevas claves estén disponibles, no así su reconocimiento por terceros.

[10] OVR-6.4.8-13 de ETSI EN 319 411-1

Cualquier fallo en la consecución de las metas marcadas por este Plan de contingencias, será tratado como razonablemente inevitable a no ser que dicho fallo se deba a un incumplimiento de las obligaciones de la AC para implementar dichos procesos.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
No aplicable para este ámbito.

5.7.3 Compromiso de la clave privada de la entidad

En caso de sospecha o conocimiento del compromiso de la AC CGCOM, se activarán los procedimientos de compromiso de claves, dirigidos por un equipo de respuesta que evaluará la situación, desarrollará un plan de acción, que será ejecutado bajo la aprobación de la dirección de la Entidad de Certificación.

En caso de compromiso de la clave privada de la AC CGCOM puede darse el caso que los estados de los certificados y de los procesos de revocación usando esta clave, podrían no ser válidos, por lo que todos los certificados emitidos y firmados con dicha clave, serán revocados, informando de tal circunstancia a través del protocolo OCSP, que devolverá el estado revoked para todos los certificados emitidos bajo esa clave, durante todo el tiempo necesario hasta que hubiese expirado el último de los certificados emitidos.

5.7.4 Continuidad del negocio después de un desastre

Dominio de creación de certificados
El proveedor técnico restablecerá los servicios críticos (revocación y publicación de certificados revocados) de acuerdo con el plan de contingencias y continuidad de negocio existente restaurando la operación normal de los servicios anteriores en las 24 horas siguientes al desastre.
Existe un Plan de Contingencias que define las acciones a realizar, recursos a utilizar y personal a emplear en el caso de producirse un acontecimiento intencionado o

accidental que inutilice o degrade los recursos y servicios de certificación prestados por VÍNTEGRIS.
Los principales objetivos del Plan de Contingencia son:
· Conseguir la mayor efectividad de las operaciones de recuperación mediante el establecimiento de tres fases: o Fase de Valoración /Activación, para detectar, evaluar los impactos y activar el plan.
Fase de Recuperación, para restablecer temporal y parcialmente los servicios hasta la recuperación de los daños provocados en el sistema original.
Fase de Reasunción, para restaurar el sistema y los procesos a su operativa habitual.

· Identificar las actividades, recursos y procedimientos necesarios para la realización eficiente y eficaz de las tres fases.

El proveedor técnico dispone de alternativas, en caso de ser necesario, para la puesta en funcionamiento de los sistemas de certificación descritos en el plan de continuidad de negocio.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.
La AC-CGCOM dispone de un plan de desastre para este ámbito.

5.8 Terminación del servicio

Dominio de creación de certificados
El proveedor técnico asegura que las posibles interrupciones a suscriptores y terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, asegura un mantenimiento continuo de los registros requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.
Antes de terminar sus servicios, el proveedor técnico desarrolla un plan de terminación con las siguientes provisiones:

- Proveerá de los fondos necesarios (mediante seguro de responsabilidad civil y provisión de fondos propios) para continuar la finalización de las actividades de revocación.
- Informará a todos los Firmantes/Suscriptores, Tercero que confían y otras AC's con las cuales tenga acuerdos u otro tipo de relación del cese con una anticipación mínima de 6 meses.
- Revocará toda autorización a entidades subcontratadas para actuar en nombre de la AC en el procedimiento de emisión de certificados.
- Transferirá sus obligaciones relativas al mantenimiento de la información del registro y de los logs durante el periodo de tiempo indicado a suscriptores y usuarios.
- Destruirá o deshabilitará para su uso las claves privadas de la AC.
- Mantendrá los certificados activos y el sistema de verificación y revocación hasta la extinción de todos los certificados emitidos.
- Emitirá la última CRL antes del cese del servicio
- Ejecutará las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en los certificados.
- Comunicará al Supervisor Nacional, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere su gestión y a quién o si se extinguirá su vigencia.
- Comunicará, también al Supervisor Nacional, la apertura de cualquier proceso concursal que se siga contra el proveedor técnico así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

Dominio de registro de usuarios y, cuando sea necesario, gestión de tarjetas por entidad interna.

La Autoridad de Certificación del CGCOM, en las instalaciones de la entidad interna, asegura que las posibles interrupciones a los suscriptores y a terceras partes son mínimas como consecuencia del cese de los servicios del prestador de servicios de certificación y, en particular, aseguran un mantenimiento continuo de los registros

requeridos para proporcionar evidencia de certificación en caso de investigación civil o criminal, mediante su transferencia a un depósito notarial.

Antes de terminar sus servicios, la Autoridad de Certificación, en la entidad interna, desarrolla un plan de terminación, con las siguientes provisiones:

- Ejecución de las tareas necesarias para transferir las obligaciones de mantenimiento de la información de registro y los archivos de registro de eventos durante los períodos de tiempo respectivos indicados al suscriptor y a los terceros que confían en certificados.

- Comunicará al Supervisor Nacional, con una antelación mínima de 2 meses, el cese de su actividad y el destino de los certificados especificando si se transfiere la gestión y a quién o si se extinguirá su vigencia.

- Comunicará, también al Supervisor nacional, la apertura de cualquier proceso concursal que se siga contra la AC-CGCOM así como cualquier otra circunstancia relevante que pueda impedir la continuación de la actividad.

6 Controles de seguridad técnica

La Autoridad de Certificación del CGCOM emplea sistemas y productos fiables, protegidos contra toda alteración y que garantizan la seguridad técnica y criptográfica de los procesos de certificación a los que sirven de soporte.

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves de las entidades de certificación intermedias son creados por la entidad de certificación raíz "vinCAsign Qualified Authority", de acuerdo con los procedimientos de ceremonia del proveedor técnico, dentro del perímetro de alta seguridad destinado a esta tarea.
Las actividades realizadas durante las ceremonias de generación de claves han sido registradas, fechadas y firmadas por todos los individuos participantes en las mismas, ante la presencia de un Notario o un Auditor. Dichos registros son custodiados a efectos de auditoría y seguimiento durante un período apropiado determinado por el proveedor técnico.

Para la generación de la clave de las entidades de certificación raíz e intermedia se utilizan dispositivos con las certificaciones FIPS 140 level 3 o Common Criteria EAL 4+ (con la aumentación ALC_FLR.1).

vinCAsign QUALIFIED Authority	**4.096 bits**	**25 Años**
SUBCA CONSEJO GENERAL DE COLEGIOS DE MÉDICOS	**4.096 bits**	**13 Años**

Más información en las siguientes direcciones web:

Texto de divulgación o PDS	https://psc.cgcom.es/pds

6.1.1.1 Generación del par de claves del firmante/suscriptor

Las claves del Firmante/Suscriptor pueden ser creadas por él mismo mediante dispositivos hardware o software autorizados por la AC CGCOM o pueden ser creadas por la AC CGCOM**.**
Las claves son generadas usando el algoritmo de clave pública **SHA-2**.
Las claves tienen una longitud mínima de **2048 bits**.

El dispositivo usado para la generación de claves deberá estar certificado de acuerdo a los requerimientos del anexo 2 del Reglamento (UE) 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de julio de 2014

Para mantener el punto anterior, el proveedor técnico establece el procedimiento interno de "**VinCASIGN Gestion validez dispositivos"**.

Cuando la AC-CGCOM distribuya los dispositivos cualificados de creación de firma, verifica en todo momento que dichos dispositivos continuan certificados como un DCCF[11].
La verificación de la certificación del DCCF se realiza durante todo el período de validez del certificado[12]. Si el DCCF perdiera su certificación como tal, la AC-CGCOM avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos.
Las claves del firmante en el servicio de firma remota son creadas por la AC-CGCOM y se generan bajo control único del firmante por medio de su PIN de activación de firma. Se usa el algoritmo de clave pública RSA con una longitud mínims de 2048 bits. Se protegen mediante el PIN de activación de firma, sobre el que se aplica el algoritmo PBKDF2 para derivación de claves.
Las claves se generan utilizando HSMs con certificación FIPS 140-2 L3 y Common Criteria EAL4+ AVA_VAN.5 que actúan como hardware criptográfico.

[11] SDP-6.5.1-02 de ETSI 319 411-2
[12] Ap 6.5.1.c) de ETSI EN 319 411-2

6.1.2 Envío de la clave privada al suscriptor

En certificados en tarjeta criptográfica

La clave privada del suscriptor se le entrega debidamente protegida mediante la entrega de la tarjeta criptográfica indicada anteriormente.

La preparación de la tarjeta es controlada de forma segura por la Autoridad de Certificación del CGCOM. La tarjeta es almacenada y distribuida de forma segura por la Autoridad de Certificación del CGCOM, como se indica en la sección 4.4, y la desactivación y reactivación de la tarjeta se controla de forma segura.

En certificados en NUBE

En certificados en dispositivo cualificado de creación de firma la clave privada se encuentra debidamente protegida en el interior de dicho dispositivo bajo el exclusivo control del titular se gestiona desde la plataforma electrónica.

6.1.3 Envío de la clave pública al emisor del certificado

El método de remisión de la clave pública al prestador de servicios de certificación es PKCS #10, otra prueba criptográfica equivalente o cualquier otro método aprobado por la Consejo General de Colegios Oficiales de Médicos .

Cuando las claves se generan en un DCCF, la AC-CGCOM se asegura que la clave pública que se remite al prestador de servicios de certificación proviene de un par de claves generadas por dicho DCCF[13].

6.1.4 Distribución de la clave pública del prestador de servicios de certificación

Las claves de la Autoridad de Certificación del CGCOM son comunicadas a los terceros que confían en certificados, asegurando la integridad de la clave y autenticando su origen, mediante su publicación en el Depósito.

[13] Ap 6.5.1.b) de ETSI EN 319 411-2

Los usuarios pueden acceder al Depósito para obtener las claves públicas, y adicionalmente, en aplicaciones S/MIME, el mensaje de datos puede contener una cadena de certificados, que de esta forma son distribuidos a los usuarios.

El certificado de la AC y su fingerprint (huella digital) estarán a disposición de los usuarios en la página Web de la AC CGCOM

6.1.5 Tamaños de claves

La longitud de las claves de la Entidad de Certificación raíz "vinCAsign Qualified Authority" es de 4096 bits.
La longitud de las claves de la Autoridad de Certificación del CGCOM es de 4096 bits.
Las claves de los subscriptores de certificados son de 2048 bits.

6.1.6 Generación de parámetros de clave pública

La clave pública de la CA Root, de la CA subordinada y de los certificados de los suscriptores está codificada de acuerdo con RFC 5280.

De acuerdo con el apartado 4.2.4 de la ETSI EN 319 412-2 al respecto de los certificados emitidos a personas físicas, se indica que en caso de incluirse, el tamaño de los campos `givenName`, `surname`, `pseudonym`, `commonName`, `organizationName` y `organizationalUnitName` puede ser más largo que el límite establecido en la IETF RFC 5280.

De acuerdo con el apartado 4.2.1 de la ETSI EN 319 412-3 al respecto de los certificados emitidos a personas jurídicas, se indica que en caso de incluirse, el tamaño de los campos `organizationName`, `organizationalUnitName` y `commonName` puede ser más largo que el límite establecido en la IETF RFC 5280.

6.1.7 Comprobación de calidad de parámetros de clave pública

- Longitud del Módulo = 4096

- Algoritmo de generación de claves: rsagen1
- Método de relleno: emsa-pkcs1-v1_5
- Funciones criptográficas de Resumen: SHA-1, SHA256.

Los algoritmos permitidos en el servicio de firma remota (SSASC) para su uso por las claves generadas a traves de dicho servicio son:

- RSA-PKCS#1v1_5
- sha256-with-rsa
- sha512-with-rsa

6.1.8 Generación de claves en aplicaciones informáticas o en bienes de equipo

Todas las claves se generan en bienes de equipo, de acuerdo con lo indicado en la sección 6.1.1.

6.1.9 Propósitos de uso de claves

Los usos de las claves de los certificados de las Autoridades de Certificación son, exclusivamente para la firma de certificados y de CRLs.
Los usos de las claves para todos los certificados de entidad final de firma y sello en NUBE son exclusivamente para la firma digital y el no repudio.
Los usos de las claves para todos los certificados de entidad final de firma y sello en tarjeta son exclusivamente para la firma digital, el no repudio y el cifrado.

6.2 Protección de la clave privada y controles de los módulos criptográficos

6.2.1 Estándares de módulos criptográficos

En relación a los módulos que gestionan las claves de CGCOM y de los suscriptores de certificados de firma electrónica, se asegura el nivel exigido por los estándares indicados en las secciones anteriores.

Los módulos criptográficos se someten a los controles de ingeniería previstos en las normas indicadas a lo largo de esta sección.
Los algoritmos de generación de claves empleados se aceptan comúnmente para el uso de la clave a que están destinados.
Todas las operaciones criptográficas del proveedor técnico son realizadas en módulos con las certificaciones FIPS 140 level 3 o Common Criteria EAL 4+ (con la aumentación ALC_FLR.1).

6.2.1.1 Hardware criptográfico para la CA Raíz "vinCAsign QUALIFIED Authority"

La clave del certificado de la autoridad de certificación raíz "vinCAsign Qualified Authority" se almacena en el HSM de Realsec "Cryptosec 2048 by Realia Technologies S.L"

6.2.1.2 Hardware criptográfico para la SubCA "CGCOM Authority"

La clave del certificado de la autoridad de certificación subordinada "CGCOM Authority" se almacena en el HSM de Primekey "SafeGuard® CryptoServer Se de Utimaco IS GmbH".

6.2.1.3 Hardware criptográfico para las claves de los certificados

Las claves privadas de los certificados emitidos en NUBE para los subscriptores, se generan en los HSM "nShield Connect XC", que cuentan con la certificación Common Criteria EAL 4+ AVA_VAN 5

Las claves privadas de los certificados emitidos en tarjeta para los subscriptores, se generan en las tarjetas cryptograficas BIT4ID

6.2.2 Control por más de una persona (n de m) sobre la clave privada

Se requiere un control multi-persona para la activación de la clave privada de la AC. En el caso de esta DPC, en concreto existe una política de 2 de 5 personas para la activación de las claves.

Los dispositivos criptográficos se encuentran protegidos físicamente tal y como se determina en este documento.

Las instalaciones de la AC están provistas de sistemas de monitorización continua y alarmas para detectar, registrar y poder actuar de manera inmediata ante un intento de acceso a sus recursos no autorizado y / o irregular.

6.2.3 Depósito de la clave privada

La AC CGCOM no almacena ni copia claves privadas de los firmantes.

6.2.4 Copia de respaldo de la clave privada

CGCOM realiza copia de seguridad de las claves privadas de las Autoridades de Certificación que hacen posible su recuperación en caso de desastre, de pérdida o deterioro de las mismas. Tanto la generación de la copia como la recuperación de ésta precisan, al menos, de la participación de dos personas.

Estos ficheros de recuperación se almacenan en armarios ignífugos y en el centro de custodia externo.

Las claves del firmante en hardware no se pueden copiar ya que no pueden salir del dispositivo criptográfico.

6.2.5 Archivo de la clave privada

Las claves privadas de las Autoridades de Certificación son archivadas por un periodo de **10 años después de la emisión del último certificado**. Se almacenarán en archivos ignífugos seguros y en el centro de custodia externo. Al menos será necesaria la colaboración de dos personas para recuperar la clave privada de las AC en el dispositivo criptográfico inicial.

Solo en caso de certificados de cifrado el suscriptor podrá almacenar la clave privada el tiempo que crea oportuno. En este caso la AC CGCOM también guardará copia de la clave privada asociada al certificado de cifrado.

6.2.6 Introducción de la clave privada en el módulo criptográfico

Las claves privadas se generan directamente en los módulos criptográficos de producción de la Autoridad de Certificación del CGCOM, en las tarjetas colegiales o en los sistemas informáticos de los suscriptores.

6.2.7 Almacenamiento de la clave privada en el módulo criptográfico

Las claves privadas de la Autoridad de Certificación se almacenan cifradas en los módulos criptográficos de producción de la Autoridad de Certificación del CGCOM.

6.2.8 Método de activación de la clave privada

La clave privada de la Autoridad de Certificación del CGCOM se activa mediante la ejecución del correspondiente procedimiento de inicio seguro del módulo criptográfico, por las personas indicadas en la sección 6.2.2.
Las claves de la AC se activan con un proceso de m de n (2 de 5)

La activación de las claves privadas de la AC Intermedia es gestionada con el mismo proceso de m de n que las claves de la AC raíz.
La activación de las claves privadas de la AC Intermedia es gestionada por el aplicativo de gestión.

La clave privada del suscriptor se activa mediante la introducción del PIN ya sea en la tarjeta, plataforme en nube o certificado en software.

6.2.9 Método de desactivación de la clave privada

Cuando la tarjeta colegial se retira del dispositivo lector, o cuando la aplicación que la utiliza finaliza la sesión, la clave privada se desactiva y resulta necesario nuevamente la introducción del PIN para activarla de nuevo.

Para la desactivación de la clave privada de la AC-CGCOM se seguirán los pasos descritos en el manual del administrador del equipo criptográfico correspondiente, en VinCAsign.

6.2.10 Método de destrucción de la clave privada

Anteriormente a la destrucción de las claves y siempre que el suscriptor lo solicite, se emitirá una revocación del certificado de las claves públicas asociadas a las mismas.

Se destruirán físicamente o reiniciarán a bajo nivel los dispositivos que tengan almacenados cualquier parte de las claves privadas de CGCOM. Para la eliminación, se seguirán los pasos descritos en el manual del administrador del equipo criptográfico.
Finalmente se destruirán de forma segura las copias de seguridad.

6.2.11 Clasificación de módulos criptográficos

Véase la sección 6.2.1.

6.3 Otros aspectos de gestión del par de claves

6.3.1 Archivo de la clave pública

La Autoridad de Certificación del CGCOM archiva sus claves públicas de forma rutinaria, de acuerdo con lo establecido en la sección 5.5 de esta política.

6.3.2 Periodos de utilización de las claves pública y privada

Los periodos de utilización de las claves son los determinados por la duración del certificado, transcurrido el cual no pueden continuar utilizándose.

Como excepción, la clave privada de descifrado puede continuar empleándose incluso tras la expiración del certificado.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de la Autoridad de Certificación del CGCOM son generados de acuerdo con lo establecido en la sección 6.2.2 y los procedimientos de ceremonia de claves. La creación y distribución de dichos dispositivos se registra.

La Autoridad de Certificación del CGCOM genera de forma segura los datos de activación de las tarjetas colegiales.

6.4.2 Protección de datos de activación

Los datos de activación de los dispositivos que protegen las claves privadas de la Autoridad de Certificación del CGCOM son protegidos por los poseedores de los mismos, que firman un contrato reconociendo sus obligaciones.

Los datos de activación de la tarjeta colegial son distribuidos separadamente de la propia tarjeta (por ejemplo, entregándose en momentos diferentes, o por rutas diferentes, o vinculando ambos justo antes del procedimiento de entrega).

El suscriptor del certificado en software es el responsable de la protección de su clave privada, con una contraseña lo más completa posible, formada por números y letras. El suscriptor debe recordar dicha contraseña.

6.4.3 Otros aspectos de los datos de activación

Sin estipulación.

6.5 Controles de seguridad informática

El proveedor técnico emplea sistemas fiables para ofrecer sus servicios de certificación. El proveedor técnico ha realizado controles y auditorias informáticas a fin de establecer una gestión de sus activos informáticos adecuada con el nivel de seguridad requerido en la gestión de sistemas de certificación electrónica.

Respecto a la seguridad de la información, el proveedor técnico sigue el esquema de certificación sobre sistemas de gestión de la información de ISO 27001.
Los equipos usados son inicialmente configurados con los perfiles de seguridad adecuados por parte del personal de sistemas del proveedor técnico, en los siguientes aspectos:

- Configuración de seguridad del sistema operativo.
- Configuración de seguridad de las aplicaciones.
- Dimensionamiento correcto del sistema.
- Configuración de usuarios y permisos.
- Configuración de eventos de Log.
- Plan de copias de seguridad y recuperación.
- Configuración antivirus.
- Requerimientos de trafico de red.

6.5.1 Requisitos técnicos específicos de seguridad informática

Cada servidor de CGCOM incluye las siguientes funcionalidades:

- Control de acceso a los servicios de la SubCA y gestión de privilegios.
- Imposición de separación de tareas para la gestión de privilegios.
- Identificación y autenticación de roles asociados a identidades.
- Archivo del historial del suscriptor y de la SubCA y datos de auditoria.
- Auditoría de eventos relativos a la seguridad.
- Auto-diagnóstico de seguridad relacionado con los servicios de la SubCA.
- Mecanismos de recuperación de claves y del sistema de la SubCA.

Las funcionalidades expuestas son realizadas mediante una combinación de sistema operativo, software de PKI, protección física y procedimientos.
La verificación de la certificación de los dispositivos cualificados (DCCF) se realiza durante todo el período de validez del certificado. Si el DCCF perdiera su certificación como tal, CGCOM avisará a los usuarios de este hecho y ejecutará un plan de renovación de estos dispositivos.

6.5.2 Evaluación del nivel de seguridad informática

Las aplicaciones de autoridad de certificación y de registro empleadas por la Autoridad de Certificación del CGCOM son fiables.

6.5.3 Periodicidad revisión de componentes del sistema mantenidos por CGCOM

Se establece en 6 meses el intervalo máximo de revisión periódica de los sistemas de la Autoridad de Certificación de la OMC, de acuerdo con el documento "Procedimiento de configuración de sistemas".

6.6 Controles técnicos del ciclo de vida

6.6.1 Controles de desarrollo de sistemas

Las aplicaciones son desarrolladas e implementadas por la Autoridad de Certificación del CGCOM de acuerdo con estándares de desarrollo y control de cambios.
Las aplicaciones disponen de métodos para la verificación de la integridad y autenticidad, así como de la corrección de la versión a emplear.

6.6.2 Controles de gestión de seguridad

La AC CGCOM desarrolla las actividades precisas para la formación y concienciación de los empleados en materia de seguridad. Los materiales empleados para la formación y los documentos descriptivos de los procesos son actualizados después de su aprobación por un grupo para la gestión de la seguridad.
Para realizar esta función dispone de un plan de formación anual.
La AC CGCOM exige mediante contrato, las medidas de seguridad equivalentes a cualquier proveedor externo implicado en las labores de certificación.

6.6.2.1 Clasificación y gestión de información y bienes

La AC CGCOM mantiene un inventario de activos y documentación y un procedimiento para la gestión de este material para garantizar su uso.

La política de seguridad de la AC CGCOM detalla los procedimientos de gestión de la información donde se clasifica según su nivel de confidencialidad.
Los documentos están catalogados en tres niveles: PÚBLICO, USO INTERNO y CONFIDENCIAL y SECRETA/RESERVADA.

6.6.2.2 Operaciones de gestión

La AC CGCOM dispone de un adecuado procedimiento de gestión y respuesta de incidencias, mediante la implementación de un sistema de alertas y la generación de reportes periódicos.
En el documento de seguridad de la AC CGCOM se desarrolla en detalle el proceso de gestión de incidencias.
La AC CGCOM tiene documentado todo el procedimiento relativo a las funciones y responsabilidades del personal implicado en el control y manipulación de elementos contenidos en el proceso de certificación.

Tratamiento de los soportes y seguridad
Todos los soportes son tratados de forma segura de acuerdo con los requisitos de la clasificación de la información. Los soportes que contengan datos sensibles son destruidos de manera segura si no van a volver a ser requeridos.

Planificación del sistema
El departamento de Sistemas de la AC CGCOM mantiene un registro de las capacidades de los equipos. Conjuntamente con la aplicación de control de recursos de cada sistema se puede prever un posible redimensionamiento.
Reportes de incidencias y respuesta
La AC CGCOM dispone de un procedimiento para el seguimiento de incidencias y su resolución donde se registran las respuestas y una evaluación económica que supone la resolución de la incidencia.

Procedimientos operacionales y responsabilidades
La AC CGCOM define actividades, asignadas a personas con un rol de confianza, distintas a las personas encargadas de realizar las operaciones cotidianas que no tienen carácter de confidencialidad.

6.6.2.3 Gestión del sistema de acceso

La AC CGCOM realiza todos los esfuerzos que razonablemente están a su alcance para confirmar que el sistema de acceso está limitado a las personas autorizadas.
En particular:

AC General

Se dispone de controles basados en firewalls, antivirus e IDS en alta disponibilidad.

Los datos sensibles son protegidos mediante técnicas criptográficas o controles de acceso con identificación fuerte.

La AC CGCOM dispone de un procedimiento documentado de gestión de altas y bajas de usuarios y política de acceso detallado en su política de seguridad.

La AC CGCOM dispone de procedimientos para asegurar que las operaciones se realizan respetando la política de roles.

Cada persona tiene asociado un rol para realizar las operaciones de certificación.

El personal de la AC CGCOM es responsable de sus actos mediante el compromiso de confidencialidad firmado con la empresa.

Generación del certificado

La autenticación para el proceso de emisión se realiza mediante un sistema m de n operadores para la activación de la clave privada de la AC CGCOM.

Gestión de la revocación

La revocación se realizará mediante autenticación fuerte con tarjeta a las aplicaciones de un administrador autorizado. Los sistemas de logs generarán las pruebas que garantizan el no repudio de la acción realizada por el administrador de la AC CGCOM.

Estado de la revocación

La aplicación del estado de la revocación dispone de un control de acceso basado en la autenticación por certificados para evitar el intento de modificación de la información del estado de la revocación.

6.6.2.4 Gestión del ciclo de vida del hardware criptográfico

CGCOM se asegura de que el hardware criptográfico usado para la firma de certificados no se manipula durante su transporte mediante la inspección del material entregado.

El hardware criptográfico se traslada sobre soportes preparados para evitar cualquier manipulación.
CGCOM registra toda la información pertinente del dispositivo para añadir al catálogo de activos.
El uso del hardware criptográfico de firma de certificados requiere el uso de, al menos, dos empleados de confianza.
CGCOM realiza test de pruebas periódicas para asegurar el correcto funcionamiento del dispositivo.
El dispositivo hardware criptográfico solo es manipulado por personal confiable.
La clave privada de firma de CGCOM almacenada en el hardware criptográfico se eliminará una vez se ha retirado el dispositivo.
La configuración del sistema de CGCOM, así como sus modificaciones y actualizaciones son documentadas y controladas.

El proveedor técnico posee un contrato de mantenimiento del dispositivo. Los cambios o actualizaciones son autorizados por el responsable de seguridad y quedan reflejados en las actas de trabajo correspondientes. Estas configuraciones se realizarán, al menos, por dos personas confiables.

6.6.3 AC-CGCOM Evaluación del nivel de seguridad del ciclo de vida

Sin estipulación.

6.7 Controles de seguridad de red

El proveedor técnico protege el acceso físico a los dispositivos de gestión de red, y dispone de una arquitectura que ordena el tráfico generado basándose en sus características de seguridad, creando secciones de red claramente definidas. Esta división se realiza mediante el uso de cortafuegos.

La información confidencial que se trasfiere por redes no seguras, se realiza de forma cifrada mediante uso de protocolos SSL o del sistema VPN con autenticación por doble factor.

6.8 Fuentes de Tiempo

El proveedor técnico dispone de su propia fuente de tiempo, es un NTP Stratum 1 en las instalaciones del CPD de COLT Barcelona. (Modelo Meinberg LANTIME M200/GPS) con el que sincroniza todos sus servicios.

Además, el proveedor técnico tiene un procedimiento de sincronización de tiempo coordinado con el ROA Real Instituto y Observatorio de la Armada en San Fernando vía NTP.

7 Perfiles de certificados y listas de certificados revocados

7.1 Perfil de certificado

La Autoridad de Certificación del CGCOM publica sus perfiles de certificados en el Depósito.

Todos los certificados cualificados emitidos bajo esta política están en conformidad con el estándar X.509 versión 3, con la RFC 5280 y con ETSI EN 319 412-1, ETSI EN 319 412-2, ETSI EN 319 412-3 y ETSI EN 319 412-5.

7.1.1 Número de versión

La AC CGCOM emite certificados X.509 Versión 3.

7.1.2 Extensiones del certificado

Los documentos de las extensiones de los certificados se encuentran detallados en documentos independientes que pueden ser accedidos desde la página Web de la AC CGCOM.

7.1.3 Identificadores de objeto (OID) de los algoritmos

El identificador de objeto del algoritmo de firma es:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption

El identificador de objeto del algoritmo de la clave pública es:

- 1.2.840.113549.1.1.1 rsaEncryption

7.1.4 Formato de Nombres

Los certificados deberán contener las informaciones que resulten necesarias para su uso, según determine la correspondiente política.

7.1.5 Restricciones de los nombres

Los nombres contenidos en los certificados están restringidos a "Distinguished Names" X.500, que son únicos y no ambiguos
Adicionalmente se pueden establecer restricciones de nombres en relación con los certificados a la correspondiente política de autenticación, firma electrónica, cifrado o evidencia electrónica, siempre que las mismas resulten objetivas, proporcionadas, transparentes y no discriminatorias.

7.1.6 Identificador de objeto (OID) de la Política de Certificación

Todos los certificados incluyen un identificador de política de certificados bajo la que han sido emitidos partiendo de la raíz 1.3.6.1.4.1.26852, de acuerdo con la estructura indicada en el punto 1.2.1

7.1.7 Extensión del uso de las restricciones de política

Sin estipulación

7.1.8 Sintaxis y semántica de los "PolicyQualifier"

Se dispone de dos campos de PKIX policy qualifier:

a) El que contiene la URL donde se publica la Declaración de Prácticas de Confianza (CPS Pointer con el OID 1.3.6.1.5.5.7.2.1)
b) El que contiene el texto con información referente al certificado para su verificación (unotice con el OID 1.3.6.1.5.5.7.2.2)

7.1.9 Tratamiento semántico para la extensión "Certificate Policy"

Esta extensión incluye el OID de la política del certificado, así como los dos campos "policy qualifier" indicados en el apartado anterior.

7.2 Perfil de la lista de revocación de certificados

7.2.1 Número de versión

Las CRL emitidas por la AC CGCOM son de la versión 2.

7.2.2 CRL y extensiones

CRL de la CA emisora de los certificados

Campos y extensiones	Valor
Versión	V2
Emisor	DN del emisor
Fecha efectiva	Fecha UTC de la emisión
Próxima actualización	Fecha emisión + 10 días
Algoritmo de firma	Sha512RSA
Algoritmo hash de firma	SHA512
Identificador de clave de entidad emisora	Hash de la clave del emisor
Número CRL	Valor incremental
Entradas de la CRL	• Número de serie • Fecha de revocación • Código de razón

7.3 Perfil de OCSP

Según el estándar IETF RFC 6960.

7.3.1 Número de versión

Conformes con el estándar X.509 versión 3.

7.3.2 Extensiones del OCSP

Sin estipulación

8 Auditoria de conformidad

La AC CGCOM es una empresa comprometida con la seguridad y la calidad de sus servicios por ello confía en el proveedor técnico para la prestación de los servicios de certificación.

El proveedor técnico es una empresa comprometida con la seguridad y la calidad de sus servicios mediante la obtención y mantenimiento de la certificación ISO/IEC 27001:2013.

Del mismo modo, AC CGCOM se encuentra registrada como prestador cualificado de servicios de certificación aprobado por el Ministerio de Industria y sometido a las revisiones de control que este organismo considere necesarias.

Las Autoridades de Registros pertenecientes a esta jerarquía están sujetas a un proceso de auditoría interna. Estas auditorías se realizan periódicamente con una frecuencia no superior a 2 años. La frecuencia de las auditorias (1 o 2 años) a las autoridades de registro son calculadas por el número de certificados emitidos y número de operadores de registro.

8.1 Frecuencia de la auditoria de conformidad

La AC CGCOM al incorporarse en la jerarquía del proveedor técnico para la prestación de los servicios de certificación, se encuentra sometida a los controles requeridos por el proveedor técnico de manera adicional a los propios controles internos de cumplimiento y adecuación de los servicios ofrecidos.

CGCOM lleva a cabo una auditoría de conformidad anualmente, además de las auditorías internas que realiza bajo su propio criterio o en cualquier momento, debido a una sospecha de incumplimiento de alguna medida de seguridad.

8.2 Identificación y calificación del auditor

Las auditorías de la AC-CGCOM son realizadas por una firma de auditoría independiente externa que demuestra competencia técnica y experiencia en seguridad informática, en seguridad de sistemas de información y en auditorías de conformidad de servicios de certificación de clave pública, y los elementos relacionados.

8.3 Relación del auditor con la entidad auditada

Las empresas de auditoría son de reconocido prestigio con departamentos especializados en la realización de auditorías informáticas, por lo que no existe ningún conflicto de intereses que pueda desvirtuar su actuación en relación con la AC.

8.4 Listado de elementos objeto de auditoria

En cuanto a la AC-CGCOM los elementos de auditoría son:

- Que la entidad tiene un sistema de gestión que garantiza la calidad del servicio prestado.
- Que la entidad cumple con los requerimientos de la DPC y otra documentación vinculada con la emisión de los distintos certificados digitales.
- Que la DPC y demás documentación jurídica vinculada, se ajusta a lo acordado por la Autoridad aprobadora de la Política y con lo establecido en la normativa vigente.
- Que la entidad gestiona de forma adecuada sus sistemas de información

En particular, los elementos objeto de auditoría serán los siguientes:

- Procesos de la AC, ARs y elementos relacionados.
- Sistemas de información.
- Protección del centro de procesamiento de datos.
- Documentos.

8.5 Acciones a emprender como resultado de una falta de conformidad

Una vez recibido por la dirección el informe de la auditoría de cumplimiento llevada a cabo, se analizan, con la firma que ha ejecutado la auditoría, las deficiencias encontradas y desarrolla y ejecuta un plan correctivo que solvente dichas deficiencias.

Si la Autoridad de Certificación auditada es incapaz de desarrollar y / o ejecutar dicho plan o si las deficiencias encontradas suponen una amenaza inmediata para la seguridad o integridad del sistema deberá comunicar inmediatamente al Consejo General de Colegios Oficiales de Médicos y al proveedor técnico , que podrá ejecutar las siguientes acciones:

- Cesar las operaciones transitoriamente.
- Revocar la clave de la Autoridad de Certificación, y regenerar la infraestructura.
- Terminar el servicio de la Autoridad de Certificación
- Otras acciones complementarias que resulten necesarias.

8.6 Tratamiento de los informes de auditoría

Los informes de resultados de auditoría se entregan al Consejo General de Colegios Oficiales de Médicos en un plazo máximo de 15 días tras la ejecución de la auditoría.

9 Requisitos comerciales y legales

9.1 Tarifas

9.1.1 Tarifa de emisión o renovación de certificados

La Autoridad de Certificación del CGCOM ha establecido una tarifa por la emisión o por la renovación de los certificados, que se suministra oportunamente a los suscriptores.

9.1.2 Tarifa de acceso a certificados

La Autoridad de Certificación del CGCOM no ha establecido ninguna tarifa por el acceso a los certificados.

9.1.3 Tarifa de acceso a información de estado de certificado

La Autoridad de Certificación del CGCOM no ha establecido ninguna tarifa por el acceso a la información de estado de certificados.

9.1.4 Tarifas de otros servicios

Sin estipulación.

9.1.5 Política de reintegro

Los suscriptores tienen derecho al desistimiento del contrato en el plazo máximo de siete días desde la recepción del mismo, sin que el ejercicio de dicho derecho pueda ocasionar penalización alguna.

9.2 Responsabilidad financiera

La Autoridad de Certificación del CGCOM dispone de recursos económicos suficientes para mantener sus operaciones y cumplir sus obligaciones, así como para afrontar el riesgo de la responsabilidad por daños y perjuicios, según lo establecido en la ETSI

EN 319 401-1 7.12 c), en relación a la gestión de la finalización de los servicios y plan de cese.

9.2.1 Cobertura de seguro

La Autoridad de Certificación del CGCOM dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 de euros.

9.2.2 Otros activos

Sin estipulación.

9.2.3 Cobertura de seguro para suscriptores y terceros que confían en certificados

La Autoridad de Certificación del CGCOM dispone de una garantía de cobertura de su responsabilidad civil suficiente, mediante un seguro de responsabilidad civil profesional que cumple con lo indicado en el artículo 24.2.c) del Reglamento (UE) 910/2014, y con el artículo 9.3.b) de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, con un mínimo asegurado de 3.000.000 de euros.

9.3 Confidencialidad de la información

9.3.1 Informaciones confidenciales

Las siguientes informaciones son mantenidas confidenciales por la Autoridad de Certificación del CGCOM:

- Solicitudes de certificados, aprobadas o denegadas, así como toda otra información personal obtenida para la expedición y mantenimiento de certificados, excepto las informaciones indicadas en la sección siguiente.
- Claves privadas generadas y/o almacenadas por el prestador de servicios de certificación.

- Registros de transacciones, incluyendo los registros completos y los registros de auditoría de las transacciones.
- Registros de auditoría interna y externa, creados y/o mantenidos por la Autoridad de Certificación y sus auditores.
- Planes de continuidad de negocio y de emergencia.
- Política y planes de seguridad.
- Documentación de operaciones y restantes planes de operación, como archivo, monitorización y otros análogos.
- Toda otra información identificada como "Confidencial".

9.3.2 Informaciones no confidenciales

La siguiente información se considera no confidencial:

- Los certificados emitidos o en trámite de emisión.
- La vinculación del suscriptor a un certificado emitido por la Autoridad de Certificación.
- El nombre y los apellidos de la persona física identificada en el certificado, así como cualquiera otra circunstancia o dato personal del titular, en el supuesto de que sea significativa en función de la finalidad del certificado.
- La dirección de correo electrónico de la persona física identificada en el certificado, o la dirección de correo electrónico asignada por el suscriptor.
- Los usos y límites económicos reseñados en el certificado.
- El periodo de validez del certificado, así como la fecha de emisión del certificado y la fecha de caducidad.
- El número de serie del certificado.
- Los diferentes estados o situaciones del certificado y la fecha del inicio de cada uno de ellos, en concreto: pendiente de generación y/o entrega, válido, revocado, suspendido o caducado y el motivo que provocó el cambio de estado.
- Las listas de revocación de certificados (LRCs), así como las restantes informaciones de estado de revocación.
- La información contenida en los depósitos de certificados.
- Toda otra información que no esté indicada en la sección anterior.

9.3.3 Divulgación de información de suspensión y revocación

Véase la sección anterior.

9.3.4 Divulgación legal de información

La Autoridad de Certificación del CGCOM divulga la información confidencial en los casos legalmente previstos para ello.

En concreto, los registros que avalan la fiabilidad de los datos contenidos en el certificado, así como los registros relacionados con la fiabilidad de los datos y los relacionados con la operativa[14], son divulgados en caso de ser requerido para ofrecer evidencia de la certificación en caso de un procedimiento judicial, incluso sin consentimiento del suscriptor del certificado.

La Autoridad de Certificación indicará estas circunstancias en la política de intimidad prevista en la sección 9.4.

9.3.5 Divulgación de información por petición de su titular

La Autoridad de Certificación del CGCOM incluye, en la política de intimidad prevista en la sección 9.4, prescripciones para permitir la divulgación de la información del suscriptor y, en su caso, de la persona física identificada en el certificado, directamente a los mismos o a terceros.

9.3.6 Otras circunstancias de divulgación de información

Sin estipulación.

9.4 Protección de la información personal

Para la prestación del servicio, la Autoridad de Certificación del CGCOM precisa recabar y almacenar ciertas informaciones, que incluyen informaciones personales.

Tales informaciones son recabadas principalmente a través de los suscriptores, en base a la relación corporativa que les une con los poseedores de claves (colegiados, órganos colegiales, personal administrativo o custodios de certificados de persona jurídica) o directamente de los afectados, con cumplimiento estricto de las

[14] REQ-7.10-04 de la ETSI EN 319 401

condiciones para el tratamiento legítimo a que se refiere el artículo 6 Reglamento general de protección de datos, y concordantes de la LOPDGDD.

La Autoridad de Certificación recaba los datos exclusivamente necesarios para la expedición y el mantenimiento del certificado.

La Autoridad de Certificación ha desarrollado una política de intimidad y documentado en esta Declaración de Prácticas de Certificación los aspectos y procedimientos de seguridad correspondientes de conformidad con el Reglamento general de protección de datos, y la LOPDGDD.

La Autoridad de Certificación no divulga ni cede datos personales, excepto en los casos previstos en las secciones 9.3.2 a 9.3.6, y en la sección 5.8, del presente documento, en caso de terminación del servicio de certificación.

La información confiresdencial de acuerdo con la normativa en protección de datos personales, es protegida de su pérdida, destrucción, daño, falsificación y procesamiento ilícito o no autorizado, de acuerdo con las prescripciones establecidas en este documento en cumplimiento del Reglamento general de protección de datos, y la LOPDGDD.

9.5 Derechos de propiedad intelectual

9.5.1 Propiedad de los certificados e información de revocación

La Autoridad de Certificación del CGCOM es la única entidad que goza de los derechos de propiedad intelectual sobre los certificados que emita, sin perjuicio de lo derechos de los suscriptores, poseedores de claves y terceros, concediendo licencia no exclusiva para reproducir y distribuir certificados, sin coste alguno, siempre y cuando la reproducción sea íntegra y no altere elemento alguno del certificado, y sea necesaria en relación con firmas digitales y/o sistemas de cifrado dentro del ámbito de uso del certificado, y de acuerdo con la documentación que los vincula.

Adicionalmente, los certificados emitidos por la Autoridad de Certificación contienen un aviso legal relativo a la propiedad de los mismos.

Las mismas reglas resultan de aplicación al uso de la información de revocación de los certificados.

9.5.2 Propiedad de la Declaración de Prácticas de Certificación

La Autoridad de Certificación del CGCOM es la única entidad que goza de los derechos de propiedad intelectual sobre esta Declaración de Prácticas de Certificación.

9.5.3 Propiedad de la información relativa a nombres

El suscriptor y, en su caso, la persona física identificada en el certificado, conserva cualquier derecho, de existir éste, relativo a la marca, producto o nombre comercial contenido en el certificado.

El suscriptor es el propietario del nombre distinguido del certificado, formado por las informaciones especificadas en la sección 3.1.1.

9.5.4 Propiedad de claves

Los pares de claves son propiedad de los suscriptores de los certificados.

Cuando una clave se encuentra fraccionada en partes, todas las partes de la clave son propiedad del propietario de la clave.

9.6 Obligaciones y responsabilidad civil

9.6.1 Obligaciones de la Autoridad de Certificación del CGCOM

La Autoridad de Certificación del CGCOM garantiza, bajo su plena responsabilidad, que cumple con todos los requisitos establecidos en cada política de certificado para la que emite certificados, siendo el único responsable del cumplimiento de los procedimientos descritos, incluso cuando una parte o la totalidad de las operaciones se subcontratan externamente.

La Autoridad de Certificación prestar los servicios de certificación conforme con esta Declaración de Prácticas de Certificación.

Antes de la emisión y entrega del certificado al suscriptor, la Autoridad de Certificación le informa de los términos y condiciones relativos al uso del certificado, de su precio y de sus limitaciones de uso.

Este requisito se cumple mediante un "Texto divulgativo de la política de certificado o PDS (PKI Disclosure Statement)" aplicable, que cumple el contenido del anexo A de la ETSI EN 319 411-1, documento que puede ser transmitido electrónicamente, empleando un medio de comunicación duradero en el tiempo, y en lenguaje comprensible.

La AC-CGCOM comunicará de forma permanente los cambios[15] que se produzcan en sus obligaciones publicando nuevas versiones de su documentación jurídica en el apartado "Regulación" de su página web https://psc.cgcom.es.

La Autoridad de Certificación vincula a suscriptores, poseedores de claves y terceros que confían en certificados mediante el Texto de Divulgación-PDS, en lenguaje escrito y comprensible, con los siguientes contenidos mínimos:

- Prescripciones para dar cumplimiento a lo establecido en las secciones 4.5.1, 4.5.4, 9.2.
- Indicación de la política aplicable, con indicación de que los certificados no se expiden al público y de la necesidad de empleo de la tarjeta como dispositivo cualificado de creación de firma o descifrado de mensajes.
- Manifestación de que la información contenida en el certificado es correcta, excepto notificación en contra por el suscriptor.
- Consentimiento para la publicación del certificado en el depósito y acceso por terceros al mismo.
- Consentimiento para el almacenamiento de la información empleada para el registro del suscriptor, para la provisión de la tarjeta colegial/dispositivo seguro

[15] Ap 6.2.3.b) de ETSI EN 319 411-1

de creación de firma y para la cesión de dicha información a terceros, en caso de terminación de operaciones de la Autoridad de Certificación sin revocación de certificados válidos.

- Límites de uso del certificado, incluyendo las establecidas en la sección 1.4.2.
- Información sobre cómo validar un certificado, incluyendo el requisito de comprobar el estado del certificado, y las condiciones en las cuales se puede confiar razonablemente en el certificado, que resulta aplicable cuando el suscriptor actúa como tercero que confía en el certificado.
- Forma en que se garantiza la responsabilidad patrimonial de la Autoridad de Certificación.
- Limitaciones de responsabilidad aplicables, incluyendo los usos por los cuales la Autoridad de Certificación acepta o excluye su responsabilidad.
- Periodo de archivo de información de solicitud de certificados.
- Periodo de archivo de registros de auditoría.
- Procedimientos aplicables de resolución de disputas.
- Ley aplicable y jurisdicción competente.
- Si la Autoridad de Certificación ha sido declarada conforme con la política de certificación y, en su caso, de acuerdo con qué sistema.

9.6.2 Garantías ofrecidas a suscriptores y terceros que confían en certificados

La Autoridad de Certificación del CGCOM, en las condiciones generales que la vinculan con suscriptores y terceros que confían en certificados, establece y rechaza garantías, y limitaciones de responsabilidad aplicables.

La Autoridad de Certificación, como mínimo, garantiza al suscriptor:

- Que no hay errores de hecho en las informaciones contenidas en los certificados, conocidos o realizados por la Autoridad 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 del mismo.
- Que los certificados cumplen con todos los requisitos materiales establecidos de la Declaración de Prácticas de Certificación.
- Que los servicios de revocación y el empleo del Depósito cumplen con todos los requisitos materiales establecidos en la Declaración de Prácticas de Certificación.

La Autoridad de Certificación, como mínimo, garantizará 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 identificado en el mismo y que el certificado ha sido aceptado, de acuerdo con la sección 4.4.
- 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 Declaración de Prácticas de Certificación.
- La rapidez y seguridad en la prestación de los servicios, en especial de los servicios de revocación y Depósito.

Adicionalmente, la Autoridad de Certificación 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 Reglamento (UE) 910/2014, en su anexo I para certificados cualificados de firma y en su anexo III para certificados cualificados de sello electrónico.
- Que, en el caso de que genere las claves privadas del suscriptor o, en su caso, persona física identificada en el certificado., se mantiene su confidencialidad durante el proceso.
- La responsabilidad de la Autoridad de Certificación, con los límites que se establezcan.

9.7 Exención de garantía

La Autoridad de Certificación del CGCOM rechaza toda garantía que no sea legalmente exigible conforme las Leyes aplicables al servicio, excepto las contempladas en la sección 9.6.2.

9.8 Responsabilidades

9.8.1 Responsabilidades de la Autoridad de Certificación

La Autoridad de Certificación del CGCOM, en su actividad de prestación de servicios de certificación, responderá por el incumplimiento de lo establecido en la DPC, y allí donde sea aplicable, por lo que dispone la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) 910/2014.

Sin perjuicio de lo anterior, la Autoridad de Certificación del CGCOM no garantizará los algoritmos y estándares criptográficos utilizados ni responderá de los daños causados por ataques externos a los mismos, siempre que hubiere aplicado la diligencia debida según el estado de la técnica en cada momento, y hubiere actuado conforme a lo dispuesto en la presente DPC, en la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, y en el Reglamento (UE) 910/2014, donde sea aplicable.

La AC CGCOM será responsable del daño causado ante el Suscriptor y/o firmante o cualquier persona que de buena fe confíe en el certificado, siempre que exista dolo o culpa grave, respecto de:

- La exactitud de la información contenida en el certificado en la fecha de su emisión, siempre que ésta corresponda a información autenticada.
- La garantía de que la clave pública y privada funcionan conjunta y complementariamente.
- La correspondencia entre el certificado solicitado y el certificado entregado.
- Cualquier responsabilidad que se establezca por la legislación vigente aplicable.

9.8.2 Responsabilidades de la Autoridad de Registro

La autoridad de registro (RA) asumirá toda la responsabilidad en el procedimiento de identificación de los suscriptores, firmantes y creadores de sellos, y en la verificación de la identidad. Deberá seguir lo estipulado en la presente DPC o según otro procedimiento aprobado por la AC CGCOM.

Cuando la generación del par de claves no sea realizada presencialmente ante el subscriptor, firmante o creador de sellos, la RA será la responsable de su custodia hasta la correspondiente entrega.

9.8.3 Responsabilidades del suscriptor

El suscriptor es responsable de cumplir con las obligaciones estipuladas en esta DPC, y en el contrato que le vincule.

9.8.4 Delimitación de responsabilidades

La AC CGCOM no será responsable en ningún caso ante las siguientes circunstancias:

a) Estado de Guerra, desastres naturales, funcionamiento defectuoso de los servicios eléctricos, las redes telemáticas y/o telefónicas o de los equipos informáticos utilizados por el Suscriptor o por los Terceros, o cualquier otro caso de fuerza mayor.
b) Por el uso indebido o fraudulento del directorio de certificados y CRL's (Lista de Certificados Revocados) emitidos por la Autoridad de Certificación.
c) Por el uso indebido de la información contenida en el Certificado o en la CRL.
d) Por el contenido de los mensajes o documentos firmados o encriptados mediante los certificados.
e) En relación a las siguientes acciones u omisiones del Solicitante y Suscriptor:
    - Falta de veracidad de la información suministrada para emitir el certificado.
    - Retraso en la comunicación de las causas de suspensión o revocación del certificado.
f) Ausencia de solicitud de suspensión o revocación del certificado cuando proceda.
    - Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación.
    - Uso del certificado fuera de su periodo de vigencia, o cuando la AC CGCOM o la RA le notifique la revocación o suspensión del mismo.

- Extralimitación en el uso del certificado, según lo dispuesto en la normativa vigente y en la presente DPC, en particular, superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por la AC CGCOM.

g) En relación a acciones u omisiones del tercero que confía en el certificado:
   - Falta de comprobación de las restricciones que figuren en el certificado electrónico o en la presente DPC en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él.
   - Falta de comprobación de la suspensión o pérdida de vigencia del certificado electrónico publicada en el servicio de consulta sobre la vigencia de los certificados o falta de verificación de la firma electrónica.

9.8.5 Cláusula de indemnidad de suscriptor

La AC CGCOM incluye en los textos de divulgación-PDS una cláusula por la cual el suscriptor se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

- Falsedad o manifestación errónea realizada por el usuario del certificado.
- Error del usuario del certificado al facilitar los datos de la solicitud, si en la acción u omisión ha mediado dolo o negligencia con respecto a la Entidad de Certificación o a cualquier persona que confía en el certificado.
- Negligencia en la protección de la clave privada, en el empleo de un sistema fiable o en el mantenimiento de las precauciones necesarias para evitar el compromiso, la pérdida, la divulgación, la modificación o el uso no autorizado de dicha clave.
- Empleo por el suscriptor de un nombre (incluyendo nombres comunes, dirección de correo electrónico y nombres de domino), u otras informaciones en el certificado, que infrinja derechos de propiedad intelectual o industrial de terceros.

9.8.6 Cláusula de indemnidad de tercero que confía en el certificado

La AC CGCOM incluye en los textos de divulgación-PDS, una cláusula por la cual el tercero que confía en el certificado se compromete a mantener indemne a la Entidad de Certificación de todo daño proveniente de cualquier acción u omisión que resulte en responsabilidad, daño o pérdida, gasto de cualquier tipo, incluyendo los judiciales y de representación letrada en que pueda incurrir, por la publicación y uso del certificado, cuando concurra alguna de las siguientes causas:

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

9.8.7 Caso fortuito y fuerza mayor

La AC CGCOM incluye en los textos de divulgación-PDS cláusulas que limitan su responsabilidad en caso fortuito y en caso de fuerza mayor.

9.9 Indemnizaciones

9.9.1 Alcance de la cobertura

La AC CGCOM dispone de un seguro que responde de las cantidades que el CGCOM resulte legalmente obligado a pagar, hasta el límite de cobertura contratado, como resultado de cualquier procedimiento judicial en el que pueda declararse su responsabilidad, derivada de cualquier acto negligente, error u incumplimiento no intencionado de la legislación vigente entre otros, en los términos expresamente pactados con la compañía aseguradora.

9.9.2 Limitaciones de pérdidas

La AC CGCOM limita su responsabilidad mediante la inclusión de los límites de uso del certificado con la extensión qcStatements en los perfiles de los certificados.

El suscriptor podrá, si lo desea, solicitar y en su caso contratar un límite superior al indicado, asumiendo los costes adicionales que en su caso se establezcan. Además, el suscriptor y terceras partes podrán acordar bilateralmente pactos o coberturas específicas para transacciones de valor superior, manteniéndose en este caso el límite de responsabilidad de la CA citado en los párrafos anteriores.

9.10 Período de validez

9.10.1 Plazo

La DPC, y los Textos de Divulgación-PDS entran en vigor cuando se publican.

9.10.2 Sustitución y derogación de la DPC

La presente DPC, y los textos de divulgación-PDS serán derogadas en el momento que una nueva versión del documento sea publicada. La nueva versión sustituirá íntegramente el documento anterior.

9.10.3 Efectos de la finalización

Para los certificados vigentes emitidos bajo una DPC anterior, la nueva versión prevalecerá a la anterior en todo lo que no se oponga a ésta.

9.11 Notificaciones individuales y comunicaciones con los participantes

La AC CGCOM establece en el contrato con el suscriptor, los medios y plazos para las notificaciones.

De modo general, se utilizará el sitio web de la AC CGCOM para realizar cualquier tipo de notificación y comunicación general, así como el correo electrónico o postal para notificaciones y comunicaciones individualizadas.

En caso de problemas de seguridad o de pérdida de integridad que puedan afectar a una persona física o jurídica, la AC CGCOM le notificará dicha incidencia sin ningún retraso.

9.12 Cambios en las especificaciones

9.12.1 Procedimiento para los cambios

- Elementos que pueden cambiar sin necesidad de notificación

Los únicos cambios que pueden realizarse a esta política sin requerir de notificación son las correcciones tipográficas o de edición o los cambios en los detalles de contacto.

- Cambios con notificación

Los elementos de esta DPC pueden ser cambiados unilateralmente por la AC CGCOM sin preaviso. Las modificaciones pueden traer causa justificativa en motivos legales, técnicos o comerciales.

Cuando corresponda, dichas modificaciones serán notificadas al Organismo de Supervisión correspondiente, y tras su aprobación definitiva, se publicará la nueva documentación con un periodo de entrada en vigor que posibilite la posible rescisión de los suscriptores que no acepten los cambios. El momento de entrada en vigor se anunciará suficientemente en el momento de publicación de los cambios.

- Mecanismo de notificación

Todos los cambios propuestos que puedan afectar sustancialmente a los suscriptores, usuarios o terceros serán notificados inmediatamente a los interesados mediante la publicación en la Web de la AC CGCOM.

Las autoridad de registro (RA) podrán ser notificadas directamente mediante correo electrónico o telefónicamente en función de la naturaleza de los cambios realizados.

9.12.2 Período y procedimiento de notificación

Cualquier acción tomada como resultado de unos comentarios queda a la discreción de la organización responsable de la administración de las políticas.

9.12.3 Circunstancias en las que el OID debe ser cambiado

Se procederá al cambio de OID en aquellas circunstancias que se altere alguno de los procedimientos descritos en el presente documento, y que afecte directamente al modo operativo de alguna de las entidades participantes.

9.13 Reclamaciones y resolución de conflictos

La AC CGCOM establece, en el contrato de suscriptor, y en los textos de divulgación-PDS, los procedimientos de mediación y resolución de conflictos aplicables.

9.14 Normativa aplicable

La Entidad de Certificación establece, en el contrato de suscriptor y en la PDS, que la legislación aplicable a la prestación de los servicios, incluyendo la política y prácticas de certificación, es la Ley española.

- Reglamento (UE) No 910/2014 del parlamento europeo y del consejo de 23 de julio de 2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE.
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas.

- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
- 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).
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

9.15 Cumplimiento de la normativa aplicable

La AC CGCOM cumple el Reglamento (UE) 910/2014, la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza, en lo que resulte aplicable, así como el resto de la normativa relacionada en el punto anterior.
La AC CGCOM establece, en el contrato de suscriptor y en los textos de divulgación-PDS, una cláusula de jurisdicción competente, indicando que la competencia judicial internacional corresponde a los jueces españoles. La competencia territorial y funcional se determinará en virtud de las reglas de derecho internacional privado y reglas de derecho procesal que resulten de aplicación.

9.16 Otras disposiciones

9.16.1 Cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación

La AC CGCOM establece, en el contrato de suscriptor, y en los textos de divulgación-PDS, cláusulas de divisibilidad, supervivencia, acuerdo íntegro y notificación:

- En virtud de la cláusula de divisibilidad, la invalidez de una cláusula no afectará al resto del contrato.
- En virtud de la cláusula de supervivencia, ciertas reglas continuarán vigentes tras la finalización de la relación jurídica reguladora del servicio entre las partes. A este efecto, la Entidad de Certificación vela porque, al menos los requisitos contenidos en las secciones 9.6 (Obligaciones y responsabilidad), 8 (Auditoría de conformidad) y 9.3 (Confidencialidad), continúen vigentes tras la terminación del servicio y de las condiciones generales de emisión/uso.

- En virtud de la cláusula de acuerdo íntegro se entenderá que el documento jurídico regulador del servicio contiene la voluntad completa y todos los acuerdos entre las partes.
- En virtud de la cláusula de notificación se establecerá el procedimiento por el cual las partes se notifican hechos mutuamente.

9.17 Otras provisiones

Sin estipulación