Plaza de las Cortes, 11
28014 Madrid
Tel. +34 914 317 780

Política de Seguridad de la Información

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

PÚBLICO

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

Histórico de cambios

Versión	Fecha	Descripción acción	Mod.
1.0	25/09/2012	Creación del documento	*Todas*
1.1	17/05/2017	Actualización documentos	Todas
2.0	24/05/2018	Adaptación al ENS	*Todas*
2.1	24/06/2020	Reformulación de la política	*Todas*
2.2	*02/03/2022*	*Revisión auditoría ENS*	*Ap. 2, 10*
2.3	17/01/2023	Revisión aprobadores (entrada JAA)	Portada
2.4	28/02/2024	Inclusión comentarios auditoría interna y revisión formal comisión de coordinación	Todos

Elaborado por	Revisado por	Revisado por	Aprobado por
Secure&IT	Director UT – José Antonio Aguado	Responsable de Seguridad/Calidad – Teresa Echevarría	Comisión de Coordinación

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

ÍNDICE

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

1. INTRODUCCIÓN Y ALCANCE

Consejo General de Colegios Oficiales de Médicos (**en adelante CGCOM**), así como sus fundaciones:

- Fundación para la Protección Social de la Organización Médica Colegial (**FPSOMC**)
- Fundación para la Formación de la Organización Médica Colegial (**FFOMC**)
- Fundación de los Colegios Médicos para la Cooperación Internacional (**FCOMCI**)

Dependen de los sistemas TIC (Tecnologías de Información y Comunicaciones) para alcanzar sus objetivos. Estos sistemas deben ser administrados con diligencia, tomando las medidas adecuadas para protegerlos frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios, actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que los departamentos deben aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

Todos los Departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI deben cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación, deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

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

Todos los departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes.

1.1. ALCANCE

Esta política se aplica a todos los sistemas TIC de CGCOM y a todos sus usuarios, ídem para las fundaciones:

- Fundación para la Protección Social de la Organización Médica Colegial (FPSOMC)
- Fundación para la Formación de la Organización Médica Colegial (FFOMC)
- Fundación de los Colegios Médicos para la Cooperación Internacional (FCOMCI)

1.2. MISIÓN Y VISIÓN

CGCOM Es el órgano que agrupa, coordina y representa a todos los ***Colegios Oficiales de Médicos*** a nivel estatal y tiene la condición de Corporación de Derecho Público con personalidad jurídica propia y plena capacidad en el cumplimiento de sus fines.

En los siguientes enlaces disponibles en la página web de la entidad se puede encontrar información en detalle sobre los propósitos y mecanismos organizativos de CGCOM

Descripción	Enlace
¿Quiénes somos?	https://www.cgcom.es/conocenos/cgcom
Reglamento sobre el procedimiento electoral	https://www.cgcom.es/sites/main/files/files/2022-03/reglamento_procedimiento_electoral_cgcom.pdf

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

1 PRINCIPIOS BÁSICOS

1.1 PREVENCIÓN

Todos los departamentos que integran CGCOM y las fundaciones mencionadas en el apartado 1.1 deben evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, deben implementar las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todos los usuarios, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, todos los departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI deben:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

1.3. DETECCIÓN

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

1.4. RESPUESTA

Todos los departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI deben:

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

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros departamentos o en otros organismos.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

1.5. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, todos los departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

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

2 REQUISITOS DE SEGURIDAD

Esta política de seguridad se establecerá de acuerdo con los principios básicos indicados y se desarrollará aplicando los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad	CGCOM, FPSOMC, FFOMC y FCOMCI considera fundamental establecer un proceso claro y estructurado para garantizar la seguridad de la Organización. Esto implica definir roles y responsabilidades, así como implementar políticas y procedimientos de seguridad, de acuerdo al procedimiento.
b) Análisis y gestión de los riesgos	La Organización debe realizar una evaluación constante de los posibles riesgos para identificar amenazas y vulnerabilidades. Luego, se deben implementar medidas para mitigar esos riesgos y verificar el correcto seguimiento e implementación de las mismas.
c) Gestión de personal	CGCOM, FPSOMC, FFOMC y FCOMCI debe asegurarse de que el personal esté adecuadamente capacitado en seguridad, así como establecer políticas y procedimientos para garantizar el cumplimiento de las normas de seguridad por parte de todos los empleados.
d) Profesionalidad	CGCOM, FPSOMC, FFOMC y FCOMCI establece a la necesidad de contar con personal calificado y ético en todas las funciones relacionadas con la seguridad, desde la planificación hasta la implementación y el mantenimiento.
e) Autorización y control de los accesos	La Organización establece controles de acceso adecuados para garantizar que solo las personas autorizadas tengan acceso a recursos y sistemas críticos.
f) Protección de las instalaciones	CGCOM, FPSOMC, FFOMC y FCOMCI implementa medidas físicas y tecnológicas para proteger las instalaciones de la Organización contra intrusiones y amenazas externas.
g) Adquisición de productos de seguridad y contratación de servicios de seguridad	La Organización considera de especial relevancia el seleccionar cuidadosamente productos y servicios de seguridad confiables y adecuados para las necesidades específicas de CGCOM, FPSOMC, FFOMC y FCOMCI.
h) Mínimo privilegio	CGCOM, FPSOMC, FFOMC y FCOMCI establece el principio de otorgar a los usuarios solo los privilegios necesarios para realizar sus funciones, reduciendo así el riesgo de abuso o mal uso de los recursos.
i) Integridad y actualización del sistema	La Organización implementa medidas para garantizar la integridad de los sistemas y datos, así como mantenerlos actualizados con las últimas correcciones de seguridad.
j) Protección de la información almacenada y en tránsito	CGCOM, FPSOMC, FFOMC y FCOMCI debe implementar controles para proteger la información confidencial tanto mientras está en reposo como durante su transmisión.
k) Prevención ante otros sistemas de información interconectados	CGCOM, FPSOMC, FFOMC y FCOMCI considera de especial importancia tener en cuenta la seguridad de los sistemas interconectados para evitar posibles brechas de seguridad a través de estos puntos de conexión.
l) Registro de la actividad y detección de código dañino	La Organización implementa sistemas de registro y monitoreo para detectar actividades sospechosas y posibles amenazas, así como contar con medidas para identificar y mitigar código malicioso.
m) Incidentes de seguridad	CGCOM, FPSOMC, FFOMC y FCOMCI establece un plan de respuesta a incidentes para manejar de manera efectiva y rápida cualquier violación de seguridad que ocurra.
n) Continuidad de la actividad	CGCOM, FPSOMC, FFOMC y FCOMCI implementa planes de continuidad del negocio para garantizar que la Organización pueda seguir funcionando en caso de un incidente de seguridad grave

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

3 ESTRUCTURA ORGANIZATIVA DE SEGURIDAD

El documento "PR08-06 Roles y responsabilidades" establece la organización de seguridad de la Organización. En dicho documento se nombra como Responsable de Seguridad a:

- Gerencia de CGCOM

Será responsable de la coordinación de la seguridad de la información, y único punto de contacto para los todos los Departamentos que integran CGCOM, FPSOMC, FFOMC y FCOMCI en esta materia.

4 MARCO LEGAL Y REGULATORIO

CGCOM, FPSOMC, FFOMC y FCOMCI trata datos de carácter personal. El Sistema de Gestión de Privacidad, al que tendrán acceso sólo las personas autorizadas, recoge los tratamientos afectados y los responsables correspondientes.

Política de privacidad	https://www.cgcom.es/politica-privacidad

Todos los sistemas de información de CGCOM y las fundaciones mencionadas se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos personales recogidos en el mencionado Sistema.

Asimismo, el marco legal y regulatorio en el que se desarrollan las actividades queda identificado en el anexo I de esta política de seguridad

5 GESTIÓN DE RIESGOS

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- Regularmente, al menos una vez al año.
- Cuando cambie la información manejada.

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

- Cuando cambien los servicios prestados.
- Cuando ocurra un incidente grave de seguridad.

Para la armonización de los análisis de riesgos, el Comité de Seguridad establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. Dicho Comité dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal. Desarrollo de la política de seguridad de la información

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La política de uso y seguridad de los sistemas de información estará a disposición de todos los usuarios que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. Dicho documento se encontrará disponible a todos los usuarios en el repositorio corporativo.

5.1 ESTRUCTURACIÓN DE SEGURIDAD DEL SISTEMA

De acuerdo a la clasificación de activos adoptada por la Organización, la documentación de procedimientos y registros del SGSI es gestionada de acuerdo al nivel de seguridad determinado por el aprobador del documento, a saber:

Confidencial: Información de carácter restringido (primera categoría 1) que, por su contenido, tratamiento y/o ciclo de vida, deba almacenarse de forma cifrada para garantizar su integridad y confidencialidad.

Restringido: Información que contiene datos de carácter personal, datos de clientes de conocimiento no público, proyectos desarrollados por CGCOM o documentación a la que únicamente tiene acceso la Dirección de la Organización o ciertos miembros (claves, etc.). En caso de divulgación puede causar perjuicio a la Organización.

Uso interno: Aquella información disponible al personal de la Organización, proveedores o terceros que precisen de información de CGCOM para el desempeño de sus funciones (procedimientos, manuales, instrucciones del sistema de gestión, etc.), y que no ha sido clasificada como confidencial o pública.

Pública: Información de la página web, folletos publicitarios, presentaciones de productos y servicios, etc.

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

Antes de su aprobación, un documento debe ser revisado para asegurar que el contenido del mismo se ajusta a lo que tiene que ser y que su formato y codificación son correctos.

En función del registro/procedimiento contemplado, la cadena de aprobación contempla varias posibilidades:

- Para documentos de aplicación integral o aquellos requeridos por el marco normativo ISO27001:2013 o ENS, la aprobación formal se realiza por parte de la Comisión de Coordinación.
- Para documentos y registros relativos al funcionamiento del SGI, la aprobación formal se realiza por parte del Responsable de Seguridad.

La revisión de un procedimiento o registro la realiza la Responsable de Seguridad de la información, la Coordinadora de UT o el Área de UT, en función de su naturaleza

En el momento de la revisión debe asegurarse que el nº de revisión o índice del documento es el correcto.

Después de la revisión el documento puede pasar a aprobación por el dueño del proceso o del director del área correspondiente al ámbito de aplicación principal del documento. En caso de documentos de aplicación integral, la aprobación corresponde a la Comisión de Coordinación.

La función que aprueba un documento es responsable de su control, actualizaciones posteriores, conservación y paso a estado obsoleto según se recoge en el procedimiento PR07-01 Control de la documentación.

6 OBLIGACIONES DE LOS USUARIOS

Todos los miembros de CGCOM, FPSOMC, FFOMC y FCOMCI y las fundaciones definidas en el alcance tienen la obligación de conocer y cumplir la Política de Seguridad de la Información y la política de uso y seguridad de los sistemas de información, siendo responsabilidad del Comité de Seguridad de la Información disponer los medios necesarios para que la información llegue a los afectados.

Todos los miembros de CGCOM, FPSOMC, FFOMC y FCOMCI con responsabilidad sobre la información atenderán a una sesión de concienciación en materia de seguridad TIC al menos una vez al año. Se establecerá un programa de

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

concienciación continua para atender a todos los miembros previamente indicados.

Los usuarios con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

Todos los usuarios deberán obedecer lo indicado en el documento política de uso y seguridad de los sistemas de información.

7 TERCERAS PARTES

Cuando CGCOM, FPSOMC, FFOMC y FCOMCI preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad creados y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando CGCOM, FPSOMC, FFOMC y FCOMCI utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que ataña a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias. Se garantizará que el personal de terceros está adecuadamente concienciado en materia de seguridad, al menos al mismo nivel que el establecido en esta Política.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

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

8 APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Comisión de Coordinación en revisión por dirección del 28 de febrero de 2024.

Esta Política se Seguridad de la Información es efectiva desde su fecha de publicación y hasta que sea reemplazada por una nueva Política.

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

9 ANEXO I: MARCO LEGAL Y REGULATORIO APLICABLE

LEGISLACION	AMBITO DE APLICACIÓN
Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.	España
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	Europa
Ley Orgánica 3/2018 de 5 de diciembre de Protección de Datos de Carácter Personal y garantía de los derechos digitales.	España
Real Decreto 1720/2007, de 21 de diciembre	España
Instrucción 1/1996, de 1 de marzo, de la Agencia de Protección de Datos, sobre ficheros automatizados establecidos con la finalidad de controlar el acceso a los edificios.	España
Código Penal art. 199 su sucesivos	España
Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia	España
Ley 24/2015, de 24 de julio, de Patentes.	España
Reglamento (UE) 910/2014 del parlamento Europeo y del Consejo de 23 de julio de 2014, relativo a la identificación electrónica y a los servicios de confianza para las transacciones electrónicas en el mercado interior.	Europa
Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.	España
Directiva 1999/93/CE, por la que se establece un marco comunitario para la firma electrónica	Europa

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

LEGISLACION	AMBITO DE APLICACIÓN
Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.	España
ETSI EN 319 401 General Policy Requirements for Trust Service Providers	Europa
ETSI EN 319 411-2 Policy and security requirements for Trust Service Providers issuing certificates: Requirements for trust service providers issuing EU qualified certificates [QCP-n-qcsd, QCP-l-qscd]	Europa
ETSI TS 119 431-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev	Europa
ETSI EN 301 549 Accessibility requirements for ICTproducts and services	Europa
Real Decreto Legislativo 8/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley General de la Seguridad Social.	España
Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores.	España
Ley 34/2002, de 11 de julio, de servicios de la sociedad de la Información y Comercio Electrónico	España
Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias	España