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	Páginas
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*
3.0	24/06/2020	Reformulación de la política	*Todas*

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 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.

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

1.2. 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.

1.3. RESPUESTA

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

- 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).

1.4. 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. 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.

3. DATOS DE CARÁCTER PERSONAL

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.

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

4. 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.
- 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

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

recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

5. 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.

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 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.

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

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.

8. APROBACIÓN Y ENTRADA EN VIGOR

Texto aprobado por la Comisión Permanente reunida el día 15 de julio de 2020.

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