POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

1. APROBACIÓN Y ENTRADA EN VIGOR

Documento aprobado el día 29 de mayo de 2019 por la Junta de Gobierno del Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid.

2. INTRODUCCIÓN

El Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid depende 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. Los diferentes departamentos 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. Los departamentos deben estar preparados para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1. PREVENCIÓN

Los departamentos 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 los departamentos 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 todo el personal, deben estar claramente definidos y documentados. Para garantizar el cumplimiento de la política, los departamentos 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.

2.2. 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.

2.3. RESPUESTA

Los departamentos del Colegio 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).

2.4. RECUPERACIÓN

Para garantizar la disponibilidad de los servicios críticos, los departamentos deben desarrollar planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3. ALCANCE

Esta política se aplica a todos los sistemas TIC del Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid y a todo el personal y miembros de la Junta de Gobierno, sin excepciones.

4. MISIÓN

Los objetivos del Colegio son:

1. Ordenación del ejercicio y representación exclusiva del mismo.
2. Defensa de los derechos e intereses profesionales.
3. Formación profesional permanente.
4. Control deontológico y aplicación del régimen disciplinario en garantía de la sociedad.
5. Promoción a nivel científico, cultural, económico y social.
6. Colaboración en el funcionamiento y mejora de las distintas administraciones

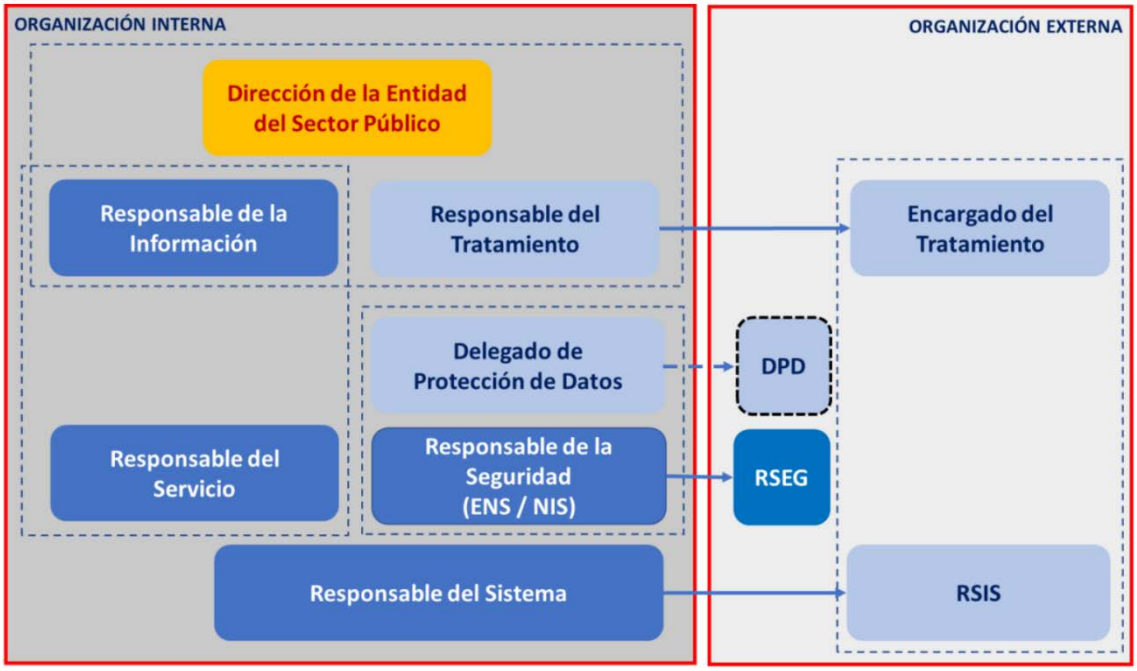
5. MARCO NORMATIVO

- Código Deontológico
- Ley 10/1997 de creación del Colegio Profesional de Fisioterapeutas
- Estatutos BOCM nº 207, 30 de agosto de 2012
- Modificación Estatutos BOCM nº 177, 27 de julio de 2017
- Ley 19/1997 de Colegios Profesionales Comunidad de Madrid
- Ley 2/1974, de 13 de febrero, sobre Colegios Profesionales
- LEY 44/03 de Ordenación De Las Profesiones Sanitarias
- LEY 25/2009: Ley sobre el libre acceso a las actividades de servicios y su ejercicio.
- LEY 2/2007 de Sociedades Profesionales

6. ORGANIZACIÓN DE LA SEGURIDAD

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

6.1. FUNCIONES Y RESPONSABILIDADES



1. Funciones del/a Responsable de Información.

El/la Responsable de la Información es una persona situada en el nivel Directivo de la organización. Esta figura tiene la responsabilidad última del uso que se haga de una cierta información y, por tanto, de su protección. El Responsable de la Información es el responsable último de cualquier error o negligencia que conlleve un incidente de confidencialidad o de integridad (en materia de protección de datos) y de disponibilidad (en materia de seguridad de la información).

2. Funciones del/a Responsable del Servicio.

El/la Responsable del Servicio establece los requisitos del servicio en materia de seguridad.

3. Funciones del/a Responsable de Seguridad.

El/la Responsable de Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios. Por un lado, mantiene la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización, por otro lado, promueve la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.
Debe reportar directamente a la Junta de Gobierno.

4. Funciones del/a Responsable del Sistema.

Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.

Sus funciones más significativas son:

a. La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al sistema de información.

b. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del sistema de información.

c. La gestión de las autorizaciones y privilegios concedidos a las personas que utilizan el sistema, incluyendo la monitorización de que la actividad desarrollada en el sistema se ajusta a lo autorizado.

d. La aplicación de los Procedimientos Operativos de Seguridad.

e. Asegurar que los controles de seguridad establecidos son adecuadamente observados.

f. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información.

g. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes.

h. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema.

i. Informar al/la Responsable de la Seguridad o al/la Responsable del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad.

j. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución.

Reportará al/la Responsable de la Seguridad en materia de seguridad, en particular, en lo relativo a decisiones de arquitectura del sistema y le entregará un resumen consolidado de los incidentes de seguridad, y al/la Responsable de la Información o al/la Responsable del Servicio de las incidencias funcionales relativas a la información que le compete.

6.2. PROCEDIMIENTOS DE DESIGNACIÓN

El/la Responsable de Seguridad de la Información recaerá en la misma persona que el/la Responsable del Servicio, siendo propuesta para estas funciones a la Gerencia. Ambos puestos deberán ser nombrados por la Junta de Gobierno y se revisará cada 2 años o cuando el puesto quede vacante.

El Responsable de Seguridad recaerá en la misma persona que el Delegado de Protección de Datos y su nombramiento se realizará por la Junta de Gobierno. La duración del primero irá ligado a la duración en el puesto del segundo o cuando el puesto quede vacante.

El/la Responsable de Seguridad deberá ser alguien con conocimientos y experiencia de IT, y podrá ser un miembro externo a la organización. Su nombramiento se realizará por la Junta de Gobierno

6.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Será misión del/la Responsable de Seguridad la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por la Junta de Gobierno y difundida para que la conozcan todas las partes afectadas.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

7. DATOS DE CARÁCTER PERSONAL

El Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid es el Responsable del Tratamiento de los datos de carácter personal que trate y deberá tratar cada dato de acuerdo a lo establecido en el Registro de actividades de tratamiento, que se hará público en la página web del Colegio. El análisis de riesgos y las medidas de seguridad aplicadas solo serán accesibles por las personas autorizadas. Todos los sistemas de información 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 Documento de Seguridad.

8. 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 o cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el Comité de Seguridad TIC establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados.

El Comité de Seguridad TIC dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

9. DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Esta Política de Seguridad de la Información complementa las políticas de seguridad del Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid en diferentes materias: Listar referencias a otras políticas en materia de seguridad.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular, para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible e impresa en Gerencia

10. OBLIGACIONES DEL PERSONAL

Toda la plantilla del Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid y los miembros de la Junta de Gobierno tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del Responsable de la Información disponer los medios necesarios para que la información llegue a los afectados. Se establecerá un programa de concienciación continua para atender a la plantilla y miembros de la Junta de Gobierno, en particular, a los/las de nueva incorporación. Las personas 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.

11. TERCERAS PARTES

Cuando el Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid 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 con el Responsable de Seguridad y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad. Cuando el Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid 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.

14. APROBACIÓN

Este documento es aprobado formalmente por la Junta de Gobierno del Colegio Profesional de Fisioterapeutas de la Comunidad de Madrid y tendrá carácter imperativo sobre toda la organización.