Centro de soporte

Servicio Murciano de Salud

Frontal Único de Gestión de Servicios de Tecnologías de la Información

POLITICA DE SEGURIDAD

Subdirección General de Tecnologías de la Información

DOCUMENTO / ARCHIVO

Titulo	Política de Seguridad	Detalle/Asunto	Política
Nombre archivo	DG_11.01 Politica de Seguridad.docx	Soporte lógico	Documento
Cliente	Servicio Murciano de salud	Localización	Gestor Documental

CONTROL DEL DOCUMENTO

Preparado por	Revisado por	Aprobado por	Autorizado por
Jose Enrique Pacheco Responsable de N2 Sistemas y Aplicaciones	Rebeca Miralles Juan Responsable de Calidad y Mejora Continua	Antonio Caravaca Moledo Responsable Técnico del Centro de Soporte	José Hernández Caravaca Director del Centro de Soporte

Índice de Contenidos

Índice de Figuras y Tablas

1 Objeto y Alcance

El Comité de Dirección del Centro de Soporte reconoce como **activos estratégicos** la información y los sistemas que la soportan, por lo que manifiesta su determinación en alcanzar los niveles de seguridad necesarios que garanticen su protección.

El objeto de la Política de Seguridad de la Información es proporcionar las directrices para **garantizar la seguridad** de la información y mejorar la calidad de los servicios que el Centro de Soporte ofrece a su cliente el Servicio Murciano de Salud.

Esta política abarca a toda la información utilizada por el Centro de Soporte, para el desarrollo de sus actividades y es aplicable, con carácter obligatorio, para el personal de que presta servicios en el Centro de Soporte, así como a las entidades colaboradoras involucradas en la utilización de la información y los sistemas.

Las relaciones con dichas **entidades colaboradoras** deben estar amparadas siempre por los contratos de prestación de servicios correspondientes, incluyendo cláusulas de **garantías** en el uso de la información.

La política de seguridad será de aplicación en todas las fases del ciclo de vida de los datos: generación, distribución, almacenamiento, procesamiento, transporte, consulta y destrucción; y de los sistemas que los procesan: análisis, diseño, desarrollo, implantación, explotación y mantenimiento.

Esta política persigue la adopción de acciones destinadas a preservar las tres componentes básicas de la seguridad aplicadas a la información:

Confidencialidad, Integridad y Disponibilidad.

2 Definiciones

- **Confidencialidad:** dimensión de la seguridad de la información que garantiza que a la información (datos y sistemas) lleguen sólo las personas autorizadas.

- **Integridad:** mantenimiento de las características de completitud y corrección de los datos y garantizar la exactitud de la información y de los sistemas contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

- **Disponibilidad:** garantizar que la información y los sistemas pueden ser utilizados en la forma y tiempo requeridos.

3 Desarrollo

3.1 Marco jurídico

El Centro de Soporte adquiere el compromiso de velar por el cumplimiento de la legislación vigente en materia de protección y seguridad de la información y de los sistemas, aplicable a todos sus procesos de negocio.

3.2 Organización y responsabilidades

La función de seguridad reside en el Responsable de Seguridad. Con dependencia funcional y autoridad delegada de ésta.

Los propietarios de la información, en cumplimiento de las normativas de seguridad, implantarán los controles necesarios asistidos por la organización de seguridad.

Las organizaciones depositarias de la información son responsables de la seguridad de plataformas, redes e infraestructura de los sistemas, conforme a las necesidades de seguridad que estas demanden de acuerdo a las normativas establecidas.

Todo usuario de los sistemas es responsable del uso adecuado que haga de los mismos y de cumplir con los controles establecidos.

3.3 Aplicación de la política de seguridad

Con objeto de poder aplicar las líneas de actuación expuestas en esta política, se precisa la definición, elaboración, implantación y mantenimiento de planes de seguridad, que recojan:

- El conjunto de normativas, estándares, guías y procedimientos operativos que determinen la forma adecuada de actuar en materia de seguridad.
- Los proyectos de inversión que doten de medios necesarios para la consecución de estos objetivos.
- La organización responsable de gestionar la seguridad.
- Los métodos de control, revisión y ajuste que permitan verificar el correcto funcionamiento de los Planes de Seguridad.

La elaboración de los planes de seguridad deberá acompañarse de procesos formales de análisis y gestión de riesgos que permitan implantar las soluciones idóneas, o bien asumir los riesgos asociados a las desviaciones respecto de estas soluciones.

3.4 Formación y concienciación

El método más efectivo de mejorar la seguridad es mediante la formación continuada y su incorporación a la actividad laboral.

Dentro de los planes de formación se incluirán cursos específicos sobre seguridad de la información acorde con el área destinataria: Dirección, técnicos, administradores y usuarios de los sistemas. Asimismo, se realizarán campañas de concienciación sobre seguridad dirigidas a todo el personal, proveedores y clientes del Centro de Soporte a través del medio que se considere más efectivo.

3.5 Auditoría

Los sistemas de información se someterán periódicamente a auditorías internas o externas con la finalidad de verificar el correcto funcionamiento de los planes de seguridad, determinando grados de cumplimiento y recomendando medidas correctoras.

3.6 Planes específicos

Cualquier plan específico sobre seguridad de la información deberá ajustarse a las disposiciones y recomendaciones de carácter más general y superior del presente documento.

3.7 Efectividad

La Política Corporativa de Seguridad de la Información entrará en vigor desde el mismo día de su publicación. Esta política será revisada con una periodicidad máxima bianual, y sus cambios deberán ser aprobados por la dirección de la organización.

Aprobado por:

Antonio Caravaca Moledo
Director Técnico Proyecto y Responsable del SGSTI

José Hernández Caravaca
Director Centro de Soporte

Fecha de última actualización: 24/11/2021 **Versión documental: 1.7**

Fecha de última revisión y verificación de vigencia: 02/02/2024