



SEGURIDAD DE LA

INFORMACIÓN

Este documento ha sido elaborado por Agesic (Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento).

El Marco de Ciberseguridad es un conjunto de requisitos (requisitos normativos y buenas prácticas) que se entienden necesarios para la mejora de la seguridad de la información y la ciberseguridad.

Usted es libre de copiar, distribuir, comunicar y difundir públicamente este documento, así como hacer obras derivadas, siempre y cuando tenga en cuenta citar la obra de forma específica.

Política de Seguridad de la información para instituciones de salud

|  |  |  |  |
| --- | --- | --- | --- |
| **Versión** | 3.0 | **Categoría** | Política |
| **Última actualización** | 24/05/2022 | **Estado** |  |

# Objetivo

La Dirección reconoce la importancia de identificar y proteger los activos de información de la Institución. Para ello, evitará la destrucción, divulgación, modificación, acceso y utilización no autorizada de toda información que produce y/o utiliza independientemente de su soporte, comprometiéndose a implantar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información, mediante el cual se desarrollarán los controles necesarios que permiten salvaguardar los principios de:

1. Confidencialidad: asegurar que sólo quienes estén autorizados puedan acceder a la información.
2. Integridad: asegurar que la información y sus métodos de proceso sean exactos y completos.
3. Disponibilidad: asegurar que los usuarios autorizados tengan acceso a la información cuando lo requieran

# Alcance

# Responsabilidades

La **Dirección** es responsable de apoyar la difusión de la Política de Seguridad de la Información toda vez que el Responsable de Seguridad de la Información así lo solicite y brindar los recursos necesarios para el cumplimiento de la misma.

Los gerentes y directores de las diferentes áreas de la Institución son responsables de hacer conocer y cumplir la Política de Seguridad de la Información entre sus subordinados, independientemente del cargo que desempeñen y de su situación contractual, incluyendo partes interesadas, socios de negocios o terceros.

El **personal**, sin importar su relación contractual, es responsable por la adhesión a la Política de Seguridad de la Información del SGSI de la organización.

# Descripción

La Dirección declara el cumplimiento con la normativa y legislación vigente en relación con aspectos de seguridad de la información.

Para gestionar la seguridad de la información, la Dirección conformará un Comité de Seguridad de la Información que tendrá como principal objetivo promover, difundir y apoyar la seguridad de la información, garantizando que la misma sea parte del proceso de planificación, definiendo las estrategias, así como aprobar los planes, políticas y todo aquello que incremente y mejore la seguridad de la información. Además, designará un Responsable de la Seguridad de la Información, quien se encargará de la guía, implementación, mantenimiento y revisión del Sistema de Gestión de Seguridad de la Información.

Es política de la Institución:

1. Establecer objetivos anuales con relación a la Seguridad de la Información.
2. Desarrollar un proceso de evaluación y tratamiento de riesgos de seguridad, y de acuerdo a su resultado, implementar las acciones correctivas y preventivas correspondientes, así como elaborar y actualizar el plan de acción.
3. Cumplir con los requisitos del servicio, legales o reglamentarios, y las obligaciones contractuales de seguridad.
4. Brindar concientización y formación en materia de seguridad de la información a todo el personal.
5. Contar con una política y procedimiento para la gestión de incidentes de seguridad de la información.
6. Establecer que todo el personal es responsable de reportar las violaciones a la seguridad, confirmadas o sospechadas de acuerdo con los procedimientos correspondientes.
7. Establecer los medios necesarios para garantizar la continuidad de las operaciones de la Institución, enmarcado en sistemas probados regularmente a fin de mantener todos sus procesos críticos activos.
8. Brindar las mayores garantías para salvaguardar la integridad, confidencialidad y disponibilidad de las historias clínicas, velando por la privacidad de la información sensible que está en poder de la institución, conforme la normativa vigente.

Esta Política de Seguridad de la Información se integrará a la normativa de la Institución.

# Cumplimiento

Se destaca que incumplimiento de la presente política aumenta la exposición de la información y el riesgo de tener un incidente de seguridad de la información. Ante la verificación de un incumplimiento la Dirección podrá tomar las medidas que se considere pertinentes, a efectos de darle el debido cumplimiento.

# Historial de revisiones

|  |  |  |
| --- | --- | --- |
| **Fecha de revisión** | **Responsable** | **Resumen de cambios** |
|  |  |  |

