

1. ALCANCE

La política de seguridad de la información pretende cubrir todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con el SANATORIO DE AGUA DE DIOS E.S.E, para conseguir un adecuado nivel de protección de las características de seguridad y privacidad de la información de la entidad.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad de la información del SANATORIO DE AGUA DE DIOS E.S.E, con el fin de regular y asegurar la gestión de la información al interior de la entidad.

3. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del instituto y, en consecuencia, debe ser protegido.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes al instituto.

SGSI: Sistema de Gestión de Seguridad de la Información.

4. GENERALIDADES

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de **SANATORIO DE AGUA DE DIOS E.S.E.** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos del sanatorio y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

SANATORIO DE AGUA DE DIOS E.S.E., consciente de la importancia de la información en el desarrollo de su actividad en la prestación de servicios de salud, y para asegurar la dirección estratégica de la entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del SANATORIO DE AGUA DE DIOS E.S.E
- Garantizar la continuidad del negocio frente a incidentes.

5. APLICABILIDAD

- Las políticas de seguridad de la información deben ser difundidas a través de capacitaciones y socialización sobre la importancia del manejo y su buen uso.
- Esta política aplica a todos los procesos, sus funcionarios, contratistas y terceros del SANATORIO DE AGUA DE DIOS, y la ciudadanía en general.

 <p>Sanatorio de Agua de Dios Empresa Social del Estado</p>	<p>POLITICA DE SEGURIDAD DE LA INFORMACION</p> <p>SANATORIO DE AGUA DE DIOS E.S.E.</p>	Código: SGSI-POL-001
		Versión N°. 1
		Fecha: Dic-2016
		Página N°. de 5

A continuación se establecen las 7 políticas específicas de seguridad que soportan el SGSI de **SANATORIO DE AGUA DE DIOS E.S.E.**

- Política de organización de la seguridad de la información
- Política de gestión de activos
- Política de control de acceso
- Política de seguridad física y del entorno
- Política de seguridad de las operaciones
- Política de seguridad de las comunicaciones
- Política de uso de software

Estas políticas están definidas en el manual de políticas específicas de seguridad de la información promulgado por la institución.

Responsabilidades

El Gerente del Sanatorio de Agua de Dios garantiza el apoyo para el desarrollo, implementación, aplicación, seguimiento y mejora continua, de la Política del Sistema de seguridad de información. Los diferentes procesos que conforman el mapa de procesos institucional deben adoptar y son responsables de su aplicación.

- **El Comité de Seguridad de la Información** es el encargado de la revisión y ajustes a la política de seguridad de la información, sus funciones están descritas en la resolución No. 10.36.617 de Octubre 24 de 2013, este comité es responsable de realizar la sensibilización y la adopción la interior de la entidad.
- **El Responsable del Activo de Información** estará encargado de la clasificación, mantenimiento y actualización de los activos de información y deberá registrar en el formato de inventario de activos de información. Así mismo definir los perfiles y roles que deben tener cada usuario para acceder a la información, y será el responsable de la integridad, confidencialidad y disposición del Activo que este a su cargo y su salvaguarda.
- **El Coordinador del Grupo de Talento Humano** deberá notificar a todo el personal que se incorpore a la institución en cualquier tipo de vinculación sobre las obligaciones del cumplimiento de la Política de Seguridad de la Información, así mismo de la elaboración de los compromisos de confidencialidad según el perfil y funciones de cada Servidor Público.
- **El Coordinador TICs** deberá seguir las directrices de esta política y cumplir con los requerimientos que en temas de seguridad informática se incorporen para garantizar el cumplimiento de la operación, administración, comunicación,

mantenimiento, gestión de los sistemas de información y recursos tecnológicos de la entidad.

- **El Asesor Jurídico** velara por el cumplimiento de la presente política en relación con la elaboración de los contratos u órdenes, representación judicial, tramite de conciliaciones, contestación de tutelas y derechos de petición de la entidad. Así mismo asesorara en materia jurídica en los temas de seguridad de información.
- **El Asesor de Control Interno** será responsable de la realización de auditorías en los diferentes procesos que conforman el mapa de procesos institucional sobre la aplicación y medidas que se tienen para el manejo de seguridad de información.

6. REFERENCIAS

- Manual para la implementación de la Estrategia de Gobierno en Línea en las Entidades del Orden Nacional de la República de Colombia, 2012-2015.
- Guía de elaboración de la política de seguridad y privacidad de la información. MinTIC 2016.
- Guía para la implementación de seguridad de la información en una MIPYME. MinTIC 2016.

7. CONTROL DE CAMBIOS

N° Edición	Fecha	Resumen de cambios
1	20/12/2016	Edición inicial