MACROPROCESO: APOYO
PROCESO: SISTEMAS
SUBPROCESO: SEGURIDAD EN INFORMACION
PROCEDIMIENTO: POLITICAS SEGURIDAD DE LA INFORMACION

1. IDENTIFICACIÓN DE NECESIDADES Y EXPECTATIVAS DEL CLIENTE:

PRODUCTOS	CLIENTES	NECESIDADES Y EXPECTATIVAS
Reglamento de Equipos	**Interno**	- Definir los parámetros para el cuidado de la información.
	Externo	- Conocer las diferentes herramientas tecnológicas de la ESE para darle una buena utilización.

2. OBJETIVO: Establecer las políticas de control que garanticen el buen uso de los recursos tecnológicos e informáticos de la ESE.

ALCANCE: 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.

Aplica para todos los procesos, ya sean internos o externos, relacionados con la entidad a través de contratos o acuerdos con terceros.

3. REPONSABLES: Ingeniero de Sistemas.

4. GENERALIDADES:

POLITICA DE SEGURIDAD DE INFORMACION

En cabeza de la Alta Dirección se compromete a desarrollar su gestión apoyada en un sistema de información que asegure la confiabilidad y oportunidad en la toma de decisiones, y que permita suministrar a todos los grupos de interés información en forma oportuna, completa y veraz para que puedan desempeñar eficazmente su labor. El hospital concibe que la información es uno de sus activos más importantes, por lo tanto, dispondrá de los recursos y mecanismos tecnológicos suficientes, necesarios y de mejores prácticas para la captura, almacenamiento y procesamiento de la misma, asegurando en todo momento su integridad, disponibilidad y confidencialidad

El Hospital Santa Isabel, consciente de la importancia de la información en el desarrollo de su actividad en la prestación de servicios de salud, ha establecido unos procesos específicos para garantizar la seguridad de sus sistemas de información, que cubre los activos de información que soportan todos los servicios.

Esta política ha sido aprobada por la Gerencia del con el fin de crear un marco de actuación que permita:

- Asegurar el cumplimiento de la legislación vigente y la normativa aplicable en materia de seguridad de la información.
- Alinear esta Política de Seguridad con el resto de políticas de la organización.
- Proteger la información gestionada por el Hospital contra cualquier uso indebido, prevenir posibles incidentes de seguridad y reducir el impacto potencial de estos.
- Asegurar la confidencialidad e integridad de la información manejada y su disponibilidad para los procesos de negocio que lo requieran.
- Asegurar la capacidad de respuesta ante situaciones de emergencia estableciendo Planes de Contingencia.
- Definir un sistema de gestión de incidentes de seguridad que permita detectar, analizar y corregir posibles brechas en la seguridad de la información. Para ello se ha definido y aprobado una metodología de gestión y tratamiento del riesgo que:

Identifica los activos del Hospital y el valor de éstos desde un punto de vista de la seguridad.
Identifica las posibles amenazas a estos activos y evalúa su nivel de riesgo.
Establece un plan de tratamiento de riesgos y unos controles de seguridad para reducir los niveles de riesgos determinados hasta un nivel aceptable.
Monitoriza y revisa anualmente el estado del sistema y la adecuación del análisis de riesgos efectuado.
Establece mecanismos para cuantificar y monitorizar los tipos, volúmenes e impacto de los incidentes, identificando y registrando acciones de mejora.