

	POLÍTICA GESTION DE LA TECNOLOGIA INFORMATICA	FECHA ELABORACIÓN: 30/10/2025
		FECHA ACTUALIZACIÓN:
	CODIGO:	PAGINA: 1-1
	VERSION: 1	REVISO Y APROBÓ: Comité institucional de gestión y desempeño - Acta 011 del 2025

POLÍTICA GESTION DE LA TECNOLOGIA INFORMATICA

La ESE ISABU garantiza la planeación, adquisición, implementación, uso seguro, mantenimiento, de la infraestructura tecnológica y sistemas de soporte clínico y administrativo en todos los niveles de la organización:

Esta gestión se desarrolla conforme a los estándares del Manual de Acreditación en Salud, y las recomendaciones técnicas y normativas de fabricantes, entes reguladores y organismos de control. Se articula con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG), incorporando los principios del Modelo Estándar de Control Interno (MECI) y las disposiciones legales aplicables en materia de telemedicina, seguridad del paciente, ciberseguridad y sostenibilidad tecnológica.

La gestión de la tecnológica informática del ISABU se orienta a garantizar la eficiencia, confiabilidad, trazabilidad, seguridad, disponibilidad, continuidad operativa y humanización de los servicios, mediante procesos sistemáticos de evaluación, capacitación, monitoreo, gestión de riesgos, renovación tecnológica y mejora continua. Todo ello se encuentra documentado, auditado y alineado con el direccionamiento estratégico institucional.

OBJETIVOS DE LA POLÍTICA

1. Optimizar el rendimiento y la eficiencia de los recursos tecnológicos de la organización a través de una Política de Gestión de Tecnología Informática que garantice la disponibilidad, seguridad, y actualización constante de los sistemas de información y aplicaciones, impulsando la innovación y la adaptación a la demanda del entorno tecnológico.

ESTRATEGIAS

1. Fortalecimiento de la infraestructura tecnológica

Renovar y mantener los activos tecnológicos conforme a criterios de obsolescencia, criticidad y disponibilidad presupuestal.

Implementar soluciones de alta disponibilidad y redundancia para garantizar la continuidad operativa.

2. Gestión segura y eficiente de los sistemas de información

Establecer procesos formales para adquisición, implementación, mantenimiento y actualización de sistemas y aplicaciones.

Asegurar la interoperabilidad, trazabilidad y cumplimiento normativo de los sistemas institucionales.

3. Ciberseguridad y protección de la información

Implementar políticas y controles de seguridad de la información, ciberseguridad y protección de datos personales.

4. Gestión de riesgos tecnológico

Identificar, evaluar y mitigar riesgos asociados al uso de tecnologías de la información.

Establecer procedimientos para la gestión de incidentes y monitoreo de controles de seguridad.

5. Capacitación y cultura tecnológica

Promover la formación continua del personal en buenas prácticas de uso, seguridad y operación de tecnologías.

Fomentar la apropiación de la cultura de seguridad y confiabilidad tecnológica.

INDICADORES

1. Porcentaje de incidentes de seguridad gestionados dentro del tiempo establecido.
2. Porcentaje de cumplimiento del plan de renovación tecnológica
3. porcentaje de personal capacitado en seguridad y ciberseguridad