 <small>MIN. 012007219-6</small>	SGC	Código: PR-AD-SGC-001	Versión: V.1
		Página: 1 de 5	
Fecha de Emisión: 18-08-2025	Título: Caracterización del Proceso de Gestión de TIC		
	Revisado por: PABLO BARRERA OVIEDO Coord. CALIDAD	Aprobado por: DAISY RUBIELA DEMOYA GERENTE	

Caracterización del Proceso de Gestión de TIC

E.S.E Hospital San Jorge de Ayapel


Este proceso de **Gestión de TIC** es estratégico porque soporta todos los demás procesos institucionales (asistenciales, administrativos, financieros y jurídicos) garantizando la **seguridad de la información, la continuidad de los servicios y la innovación digital** en el hospital.

1. Objetivo:

Garantizar la planeación, implementación, administración, seguridad y uso eficiente de las Tecnologías de la Información y las Comunicaciones (TIC) en el hospital, asegurando el soporte a los procesos misionales, estratégicos y de apoyo, en cumplimiento de la normatividad vigente y alineado al MIPG y al Sistema de Gestión de Calidad.

2. Alcance:

Aplica a la gestión de la infraestructura tecnológica, software, comunicaciones, seguridad de la información, sistemas de historia clínica electrónica, bases de datos, servicios en línea y demás plataformas digitales del hospital, desde la planeación hasta su monitoreo y mejora.

 <small>NTC 812001219-6</small>	SGC	Código: PR-AD-SGC-001	Versión: V.1
		Página: 2 de 5	
	Fecha de Emisión: 18-08-2025	Título: Caracterización del Proceso de Gestión de TIC	
	Revisado por: PABLO BARRERA OVIEDO Coord. CALIDAD	Aprobado por: DAISY RUBIELA DEMOYA GERENTE	

3. Norma de referencia:


- Ley 1341 de 2009 – Principios y marco general TIC en Colombia.
- Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública.
- Ley 1581 de 2012 – Protección de datos personales (Habeas Data).
- Decreto 612 de 2018 – Articulación del MIPG.
- Ley 527 de 1999 – Comercio Electrónico y firma digital.
- Decreto 1078 de 2015 – Decreto Único Reglamentario TIC.
- NTC ISO/IEC 27001 – Seguridad de la Información.
- NTC ISO 9001:2015 – Sistema de Gestión de Calidad.
- Resolución 1995 de 1999 – Manejo y custodia de historias clínicas.

4. Proveedor:

- Ministerio TIC.
- Ministerio de Salud y Protección Social.
- Proveedores de hardware, software y telecomunicaciones.
- Entidades de control y regulación.

5. Entradas:

- Normatividad vigente en materia de TIC y protección de datos.
- Necesidades tecnológicas de las áreas del hospital.
- Requerimientos de los usuarios internos y externos.
- Presupuesto asignado.
- Plan estratégico institucional y directrices de gobierno digital.

<div><div><div>E.S.E HOSPITAL</div><div>SAN JORGE DE AYAPEL</div><div>NOT. 012007219-6</div></div></div>	<div>SGC</div>	<div>Código:</div> <div>PR-AD-SGC-001</div>	<div>Versión:</div> <div>V.1</div>
		<div>Página: 3 de 5</div>	
<div>Fecha de Emisión:</div> <div>18-08-2025</div>	<div>Título:</div> <div>Caracterización del Proceso de Gestión de TIC</div>		
	<div>Revisado por:</div> <div>PABLO BARRERA OVIEDO</div> <div>Coord. CALIDAD</div>	<div>Aprobado por:</div> <div>DAISY RUBIELA DEMOYA</div> <div>GERENTE</div>	

6. Ciclo PHVA aplicado:


- **Planear:** Diseñar el plan estratégico de TIC, definir lineamientos de seguridad digital, establecer presupuesto.
- **Hacer:** Implementar y administrar sistemas informáticos, redes, aplicaciones y servicios digitales.
- **Verificar:** Monitorear indicadores de desempeño TIC, revisar accesibilidad, disponibilidad y seguridad.
- **Actuar:** Mejorar continuamente la infraestructura, actualizar sistemas y garantizar la sostenibilidad digital.

7. Actividades principales:

1. Administrar la infraestructura tecnológica (hardware, software, redes, servidores).
2. Garantizar la custodia y seguridad de la información institucional (historias clínicas, bases de datos, información administrativa).
3. Implementar políticas de gobierno digital y protección de datos personales.
4. Gestionar la mesa de ayuda y soporte técnico a usuarios internos.
5. Desarrollar e implementar proyectos tecnológicos alineados con el plan estratégico.
6. Coordinar la interoperabilidad con entidades externas (MSPS, EPS, entes de control).
7. Capacitar a los usuarios en el uso seguro y adecuado de las TIC.

8. Responsables:

- **Líder del proceso:** Coordinador o Responsable de TIC del hospital.
- Soporte técnico – equipo de sistemas.
- Responsables de áreas usuarias de sistemas de información.
- Gerencia del hospital (como órgano de decisión).


 <small>PROT. 0120071219-6</small>	SGC	Código: PR-AD-SGC-001	Versión: V.1
		Página: 4 de 5	
Fecha de Emisión: 18-08-2025	Título: Caracterización del Proceso de Gestión de TIC		
	Revisado por: PABLO BARRERA OVIEDO Coord. CALIDAD	Aprobado por: DAISY RUBIELA DEMOYA GERENTE	

9. Salidas:

- Plan Estratégico de TIC institucional.
- Infraestructura tecnológica en funcionamiento.
- Reportes de seguridad informática.
- Soporte técnico a usuarios.
- Bases de datos actualizadas y protegidas.
- Servicios digitales disponibles para usuarios internos y externos.

10. Puntos de control:

- Disponibilidad de los sistemas (tiempo en línea).
- Cumplimiento de normativas de protección de datos personales.
- Ejecución presupuestal en TIC.
- Respuesta de la mesa de ayuda a usuarios.
- Cumplimiento de políticas de seguridad digital.

 <small>PROT. 012007219-6</small>	SGC	Código: PR-AD-SGC-001	Versión: V.1
		Página: 5 de 5	
	Fecha de Emisión: 18-08-2025	Título: Caracterización del Proceso de Gestión de TIC	
	Revisado por: PABLO BARRERA OVIEDO Coord. CALIDAD	Aprobado por: DAISY RUBIELA DEMOYA GERENTE	

11. Indicadores:

- % Disponibilidad de sistemas de información (ej: historia clínica electrónica).
- % Cumplimiento de plan estratégico TIC.
- % Respuesta oportuna a incidentes técnicos.
- Nivel de satisfacción de usuarios internos con los servicios TIC.
- % Ejecución presupuestal en proyectos tecnológicos.

12. Gestión de riesgos:

- **Riesgo tecnológico:** Fallas en sistemas informáticos que interrumpan la atención en salud. → Control: Plan de contingencia y respaldo de información.
- **Riesgo de seguridad:** Pérdida, fuga o robo de datos sensibles. → Control: Políticas de ciberseguridad y respaldo periódico.
- **Riesgo financiero:** Insuficiencia de recursos para inversión tecnológica. → Control: Priorización de proyectos y gestión de recursos externos.
- **Riesgo de obsolescencia:** Tecnologías desactualizadas. → Control: Plan de renovación tecnológica.
- **Riesgo de desconocimiento del usuario:** Mal uso de herramientas digitales. → Control: Programas de capacitación.