1. OBJETIVOS

GENERAL: Establecer políticas, procesos y procedimientos para lograr la seguridad y privacidad de la información para la protección de los activos de información, los recursos y la tecnología, preservando la confidencialidad, integridad y disponibilidad de la información de la E.S.E Hospital Universitario de la Samaritana.

ESPECÍFICOS:

- Promover el uso de mejores prácticas de seguridad de la información en la institución
- Optimizar la gestión de la seguridad de la información al interior del HUS
- Fortalecer el uso de las Tecnologías de la Información al interior del HUS, desarrollando las actividades necesarias para garantizar su seguridad, monitoreo, seguimiento, control y mejora continua.
- Garantizar la seguridad y la privacidad de la información.
- Comprometer a todos los funcionarios del HUS en la formulación e implementación de controles y acciones encaminadas a prevenir los riesgos de la seguridad y privacidad de la información.

Fortalecer la cultura de seguridad y privacidad de la información en los funcionarios, contratistas, terceros, estudiantes, practicantes y proveedores.

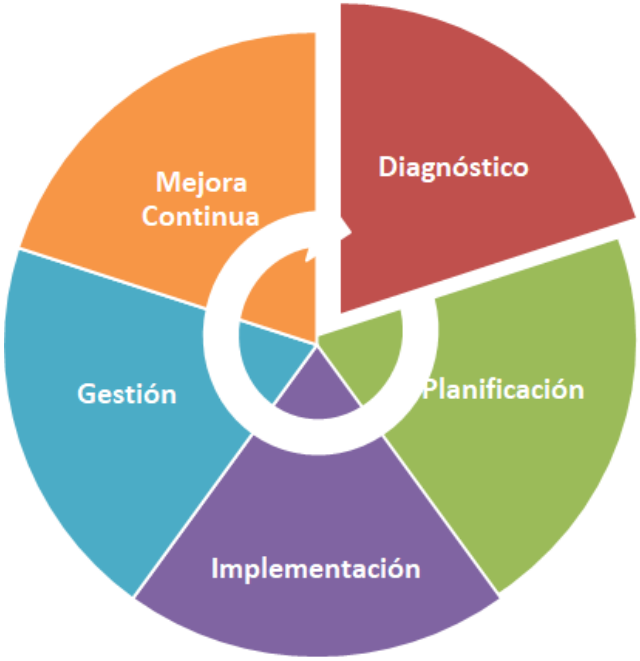
2. ALCANCE

El presente documento, está destinado a orientar a las áreas y colaboradores del HUS para la implementación de controles, adopción políticas y lineamientos que permitan preservar la confidencialidad, integridad y disponibilidad de la información que reciban, generen y procesen en medio físico o digital, con el fin de mitigar la afectación ante posibles amenazas.

Se definen las actividades a ser lideradas por el HUS durante el 2021, en cumplimiento de sus funciones y para el logro de sus objetivos.

3. METODOLOGÍA

La implementación del Sistema de gestión de seguridad y privacidad de la información, toma como base la metodología PHVA (Planear, Hacer, Verificar y Actuar), el modelo MSPI de MINTIC, el modelo integrado de planeación y gestión – MIPG y la norma ISO 27001:2013.



FASE DE DIAGNÓSTICO - ETAPAS PREVIAS A LA IMPLEMENTACIÓN: En esta fase se pretende identificar el estado actual del HUS con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información,
En la fase de diagnóstico del MSPI se pretende alcanzar las siguientes metas:

- Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- Determinar el nivel de madurez de los controles de seguridad de la información.
- Identificar el avance de la implementación del ciclo de operación al interior de la entidad.
- Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.
- Identificación del uso de buenas prácticas en ciberseguridad.

FASE DE PLANIFICACIÓN: Para el desarrollo de esta fase el HUS debe utilizar los resultados de la etapa anterior y proceder a elaborar el plan de seguridad y privacidad de la información alineado con el objetivo misional del HUS, con el propósito de definir las acciones a implementar a nivel de seguridad y privacidad de la información, a través de una metodología de gestión del riesgo.

El alcance del MSPI permite a HUS definir los límites sobre los cuales se implementará la seguridad y privacidad. Este enfoque es por procesos y debe extenderse a toda el HUS. Para desarrollar el alcance y los límites del Modelo se deben tener en cuenta las siguientes recomendaciones: Procesos que impactan directamente la consecución de objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados, e interrelaciones del Modelo con otros procesos.

FASE DE IMPLEMENTACIÓN: Esta fase le permitirá al HUS, llevar acabo la implementación de la planificación realizada en la fase anterior del MSPI.

FASE DE EVALUACIÓN DE DESEMPEÑO: El proceso de seguimiento y monitoreo del MSPI se hace con base a los resultados que arrojan los indicadores de la seguridad de la información propuestos para verificación de la efectividad, la eficiencia y la eficacia de las acciones implementadas.

FASE DE MEJORA CONTINUA: En esta fase el HUS debe consolidar los resultados obtenidos de la fase de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, tomando las acciones oportunas para mitigar las debilidades identificadas.

LÍNEAS ESTRATÉGICAS

Fortalecer a un nivel optimizado, controles del Sistema de Gestión de Seguridad de la información.

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Servicios tecnológicos, uso y apropiación
- Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz.

Implementar estrategias de sensibilización en seguridad de la información.

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Servicios tecnológicos, uso y apropiación
- Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz.

Propender por la continuidad, funcionamiento, disponibilidad de los sistemas de información misionales y de apoyo

- Componente GEL: TIC para la Gestión
- Dominios del Marco TI: Sistemas de Información, Servicios Tecnológicos, Gestión de la Información, Uso y Apropiación:
- Objetivo estratégico Institucional: Garantizar un Sistema de Información integral, eficiente y eficaz

4. ACTIVIDADES

No	QUE (ACTIVIDADES)	RESPONSABLE DEL CUMPLIMIENTO	FECHA DE CUMPLIMIENTO	DONDE	COMO Pautas para la realización de la actividad

1.	Diseñar campañas en seguridad informática	Subdirector Sistemas	31/05/2025	HUS	Diseñar y publicar campañas en temas de seguridad de la información para los clientes internos
2.	Seguimiento a los procesos de inactivación de usuarios.	Subdirector Sistemas	30/06/2025	HUS	Seguimiento al proceso de inactivación de usuarios.
3.	Seguimiento a los procesos de generación de backup.	Subdirector Sistemas	30/06/2025	HUS	Seguimiento a los procesos de generación de backup y resguardo de la información.

5. ANEXOS
Cronograma

6. CONTROL DE CAMBIOS

VERSIÓN	FECHA	ÍTEM MODIFICADO	JUSTIFICACIÓN
01	29/09/2018	N/A	Primera vez dando el cumplimiento en el decreto 612 de 2018
02	29/01/2021	Actualización de numeral 8	Actualización del plan.
03	30/01/2025	Actualización de formato	Ajuste acorde a las plantillas institucionales.