1. OBJETIVO

Adoptar la Política de Seguridad Digital expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones mediante el CONPES 3854 de 2016, cuyo objeto es fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia, contribuyendo al crecimiento de la economía digital nacional y a una mayor prosperidad económica y social en el país, garantizando al mismo tiempo la protección de los activos de información y la continuidad de los servicios de la E.S.E.

2. OBJETIVOS ESPECÍFICOS

- Establecer un marco institucional de gestión de la seguridad digital, que permita identificar, analizar, evaluar y tratar los riesgos asociados a los activos de información, sistemas de información y servicios digitales de la E.S.E.
- Fortalecer la protección de la información institucional, en especial la información clínica, administrativa y los datos personales, garantizando su confidencialidad, integridad, disponibilidad y trazabilidad, conforme a la normatividad vigente.
- Implementar controles técnicos, administrativos y organizacionales orientados a prevenir, detectar y mitigar amenazas e incidentes de seguridad digital que puedan afectar la operación institucional y la prestación de los servicios de salud.
- Definir y aplicar procedimientos para la gestión de incidentes de seguridad digital, asegurando su atención oportuna, registro, análisis y reporte a las autoridades competentes cuando corresponda.
- Promover una cultura organizacional de seguridad digital, mediante programas permanentes de sensibilización y capacitación dirigidos a servidores públicos, contratistas y colaboradores de la entidad.
- Garantizar la continuidad de los servicios institucionales y la recuperación de la información, mediante la implementación de planes de respaldo, recuperación ante desastres y continuidad del negocio para los sistemas críticos.
- Articular la seguridad digital con el Modelo Integrado de Planeación y Gestión – MIPG, la Política de Gobierno Digital y el Sistema de Control Interno, asegurando coherencia institucional y mejora continua.
- Asegurar el cumplimiento de la normatividad vigente en materia de seguridad digital y protección de datos personales, así como de los lineamientos emitidos por MinTIC y el Departamento Administrativo de la Función Pública.

3. ALCANCE

La presente política aplica a todos los procesos estratégicos, misionales, de apoyo y de evaluación de la E.S.E., así como a todos los servidores públicos, trabajadores oficiales,

contratistas, proveedores y terceros que tengan acceso a los activos de información físicos y digitales, sistemas de información, infraestructura tecnológica y servicios digitales de la entidad.

4. RESPONSABLES DE LA APLICACIÓN

- Director: Aprobar, adoptar y garantizar la implementación de la política.
- Comité Institucional de Gestión y Desempeño: Orientar, evaluar y realizar seguimiento a la política.
- Líder de Sistemas o TIC: Coordinar la implementación técnica y operativa de la política.
- Responsables de procesos: Aplicar los lineamientos de seguridad digital en sus procesos.
- Todos los servidores públicos y contratistas: Cumplir y aplicar las disposiciones de la presente política.

5. MARCO NORMATIVO

- Constitución Política de Colombia, artículos 15 y 209.
- Ley 1581 de 2012 – Protección de Datos Personales.
- Decreto 1377 de 2013 – Reglamentario de la Ley 1581 de 2012.
- Ley 1712 de 2014 – Transparencia y Acceso a la Información Pública.
- Ley 1341 de 2009 – Ley de TIC.
- Decreto 1078 de 2015 – Decreto Único Reglamentario del sector TIC.
- Decreto 612 de 2018 – Integración del MIPG.
- Decreto 767 de 2022 – Política de Gobierno Digital.
- CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- Lineamientos del Ministerio TIC y del Departamento Administrativo de la Función Pública.
- Estándares de referencia ISO/IEC 27001 e ISO/IEC 27002.

6. DESCRIPCIÓN Y / O COMPROMISO DE LA POLÍTICA

La E.S.E. se compromete a implementar y mantener un sistema de gestión de seguridad digital que permita proteger sus activos de información, gestionar adecuadamente los riesgos digitales, prevenir y atender incidentes de seguridad de la información, garantizar la continuidad de los servicios institucionales y promover el uso responsable de las tecnologías, en coherencia con los principios de legalidad, eficiencia, transparencia y responsabilidad institucional.

7. ACCIONES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

- Definir, implementar y mantener un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información alineado con los lineamientos de Gobierno Digital, el MIPG y la normatividad vigente.
- Promover programas permanentes de sensibilización y capacitación en seguridad de la información y seguridad digital dirigidos a servidores públicos, contratistas y colaboradores.

- Implementar mecanismos, procedimientos y herramientas técnicas y administrativas para prevenir, detectar, atender, controlar y mitigar incidentes de seguridad digital, garantizando la continuidad de los servicios institucionales.
- Gestionar de manera oportuna y documentada los incidentes de seguridad digital, activando los protocolos establecidos e informando a las autoridades competentes cuando corresponda.
- Fortalecer la protección de los activos de información institucionales, especialmente aquellos que contienen datos personales, datos sensibles e información clínica, mediante clasificación de la información, controles de acceso, autenticación, cifrado y respaldo.
- Implementar esquemas de copias de seguridad periódicas, planes de recuperación ante desastres y continuidad del negocio para los sistemas críticos.
- Establecer lineamientos de control de accesos lógicos y físicos a los sistemas, bases de datos, aplicaciones y equipos tecnológicos.
- Realizar evaluaciones periódicas de vulnerabilidades y revisiones de seguridad sobre la infraestructura tecnológica y los sistemas de información.
- Articular esta política con la Política de Gobierno Digital, la Política de Protección de Datos Personales y el Sistema de Control Interno.
- Mantener actualizados los procedimientos, manuales, matrices y registros asociados a la seguridad digital.

8. PARTES INTERESADAS

- Usuarios y pacientes de la E.S.E.
- Servidores públicos y contratistas.
- Proveedores de servicios tecnológicos.
- Ministerio TIC.
- Departamento Administrativo de la Función Pública.
- Ministerio de Salud y Protección Social.
- Entes de control.
- Ciudadanía en general.

9. MECANISMOS DE MEDICIÓN DE LA POLÍTICA

La Política de Seguridad Digital será objeto de seguimiento y evaluación periódica, con el fin de identificar oportunidades de mejora, asegurar su actualización y garantizar su alineación con los lineamientos del Gobierno Nacional, el sector salud y las necesidades institucionales.

INDICADOR	FÓRMULA	PERIODICIDAD	RESPONSABLE
Cumplimiento de actividades de Seguridad Digital	(Actividades ejecutadas / Actividades Programadas) x 100	Cuatrimestral	Sistemas
Resultado FURAG Seguridad Digital	Resultado cuestionario	Anual	Sistemas Planeación

10. GENERALIDADES O POLÍTICAS OPERACIONALES

- Todo acceso a los sistemas de información debe estar autorizado y registrado.
- Todo equipo institucional debe contar con software autorizado y actualizado.
- Está prohibido compartir usuarios, contraseñas o credenciales de acceso.
- La información institucional solo podrá ser utilizada para fines misionales y administrativos.
- Los incidentes de seguridad deben ser reportados de manera inmediata.
- El incumplimiento de esta política dará lugar a las acciones administrativas, disciplinarias y legales a que haya lugar.

11. DOCUMENTOS RELACIONADOS

- Política de Gobierno Digital de la E.S.E.
- Política de Protección de Datos Personales.
- Plan Estratégico de Tecnologías de la Información – PETI.
- Procedimiento de Gestión de Incidentes de Seguridad Digital.
- Matriz de Identificación y Clasificación de Activos de Información.
- Matriz de Riesgos
- Registros de capacitaciones en seguridad digital.

12. CONTROL DEL DOCUMENTO:

Z:\BIBLIOTECA HSVA\1. MANUAL DE DOCUMENTOS HSVA\3. PROCESOS DE APOYO\13. GESTION DE TIC'S\3.1 SISTEMAS DE INFORMACIÓN\POLITICAS

DATOS	**ELABORÓ**	**REVISÓ**	**APROBÓ**
Nombre	Freddy Cabrera Anaya	Ana María Ibarra	Comité Institucional de Gestión y Desempeño
Cargo	Líder Sistemas	Líder Planeación	Acta No. 006 del 2025
Fecha	29/12/2025	29/12/2025	29/12/2025

CONTROL DE CAMBIOS					
VERSION	**FECHA APROBACIÓN**			**MOTIVO**	**PARTICIPANTES ACTUALIZACIÓN**
	DIA	**MES**	**AÑO**		
01	29	12	2025	Creación del Documento	**Nombre** Freddy Cabrera Anaya **Cargo** Líder Sistemas **Nombre** Ana María Ibarra **Cargo** Líder Planeación