POLÍTICA SEGURIDAD DIGITAL

El Gerente de la Empresa Social del Estado Instituto de Salud de Bucaramanga y sus colaboradores se comprometen a implementar los tres pilares fundamentales de la seguridad de la información - confidencialidad, integridad y disponibilidad -, estableciendo un marco de confianza en el ejercicio de sus deberes con el Estado y partes interesadas, protegiendo la información, disminuyendo el impacto generado sobre sus activos, identificando los riesgos de manera sistemática con objeto de mantener un nivel de exposición aceptable, asegurando la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés y cumpliendo con los principios de la Función Administrativa.

OBJETIVO

Garantizar los tres (3) pilares fundamentales de la seguridad de la información gestionando y controlando la implementación de la seguridad digital al interior de la ESE ISABU por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, y la definición de controles para la mitigación del riesgo, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información.

OBJETIVOS ESPECÍFICOS

- Cumplir con los principios de seguridad de la información.
- Minimizar el riesgo en la seguridad de la información de los procesos misionales de la entidad.
- Apoyar la innovación tecnológica
- Establecer las políticas, procedimientos e instructivos en materia de seguridad digital
- Proteger los activos tecnológicos
- Fortalecer la cultura de seguridad de la información en los usuarios, funcionarios, ejecutores, terceros, docentes, estudiantes, proveedores y la ciudadanía en general de la E.S.E Instituto de Salud de Bucaramanga.
- Mantener la confianza de sus usuarios y colaboradores.
- Garantizar la continuidad de la prestación del servicio misional frente a incidentes de seguridad Digital.

ESTRATEGIAS DE IMPLEMENTACIÓN DE LA POLÍTICA SEGURIDAD DIGITAL

La implementación de la política por parte de la ESE ISABU se hará a través de la adopción e implementación del Modelo de Gestión de Riesgos de Seguridad Digital dispuesto en la Guía de Administración de Riesgos. De igual manera, la ESE dará cumplimiento al CONPES 3854 de 2016.

No.	Estrategia	Descripción de la Estrategia
1	Implementar y mejorar de forma continua la política de seguridad de la información.	Implementar, evaluar y mantener actualizada las políticas de seguridad de la información de la ESE ISABU
2	Salvaguardar la información de la entidad y los usuarios de los servicios prestados por la Institución	Identificar riesgos a los que se puede encontrar expuesta la información que maneja la institución en el entorno digital y así poder implementar controles para su mitigación y tratamiento.
3	Garantizar Entornos Digitales Seguro para el desarrollo de las actividades que presta la entidad	Implementación de las políticas de seguridad de la información y datos personales, promoviendo la educación y concientización de riesgos y buenas prácticas de uso de los servicios digitales,

	para el ciudadano.	

INDICADORES DE LA POLÍTICA SEGURIDAD DIGITAL

No.	Nombre del Indicador	Fórmula	Seguimiento
1	Tratamiento de eventos relacionados con la seguridad y privacidad de la información.	Número de actividades ejecutadas en el Plan de tratamiento de riesgo de seguridad / Total de actividades Programadas en el Plan de tratamiento de riesgo de seguridad	Semestral
2	Campañas educativas de seguridad de la información y protección de datos personales.	Número de Campañas educativas de seguridad de la información ejecutadas en el periodo evaluado / Total de Campañas educativas de seguridad de la información Programadas en el periodo evaluado X 100	Semestral
3	Porcentaje de Innovación tecnológica implementadas en la entidad.	Número de actividades cumplidas en el fortalecimiento de la infraestructura tecnológica de la entidad / Total de actividades Programadas en el fortalecimiento de la infraestructura tecnológica en el periodo evaluado X 100	Semestral
4	Porcentaje de Protección de los activos tecnológicos.	Número de actividades ejecutadas en actualización e Implementación de la política de seguridad de la información / Total de actividades programadas de actualización e Implementación de la política de seguridad de la información en el periodo evaluado X 100	Semestral