POLITICA DE SEGURIDAD DE LA INFORMACIÓN, CIBERSEGURIDAD Y PROTECCIÓN DE LA PRIVACIDAD

La **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** reconoce la importancia crítica de proteger la confidencialidad, integridad y disponibilidad de la información, tanto propia como de terceros, para garantizar la continuidad del negocio y la confianza de nuestros usuarios internos, externos y partes interesadas. Esta política de seguridad de la información, ciberseguridad y protección de la privacidad establece los principios, estándares y responsabilidades para proteger la información.

OBJETIVOS DE LA POLÍTICA

Establecer las políticas que regulan la seguridad de la información, ciberseguridad y protección de la privacidad en la **EMPRESA SOCIAL DEL ESTADO INSTITUTO DE SALUD DE BUCARAMANGA** y presentar en forma clara y coherente los elementos que deben conocer, acatar y cumplir todos los empleados, contratistas, proveedores y partes interesadas, con el fin de asegurar la confidencialidad, disponibilidad e integridad de la información de la entidad.

ESTRATEGIAS

1. **Seguridad desde el diseño**: Identificar requisitos, riesgos, amenazas y en enfoque en confidencialidad, integridad y disponibilidad de la información.
2. **Continuidad y gestión:** Incorporar información que contenga declaraciones relativas a:
   a) definición de seguridad de la información;
   b) Marco para establecer objetivos de seguridad de la información;
   c) lineamientos de la política de seguridad de la información de acuerdo con el modelo de seguridad y privacidad de la información MSPI
   d) compromiso de satisfacer los requisitos aplicables relacionados con la seguridad de la información;
   e) compromiso con la mejora continua del sistema de gestión de seguridad de la información;
   f) asignación de responsabilidades para la gestión de la seguridad de la información a roles definidos;
   g) procedimientos para el manejo de exenciones y excepciones.

3. **Gestión de riesgos de seguridad digital:** Definir, identificar, proyectar, valorar y tomar en consideración los requisitos derivados de los riesgos y amenazas actuales para la seguridad de la información

4. **Cultura de seguridad digital:** Fomentar la formación, sensibilización y compromiso de

de satisfacer los requisitos aplicables relacionados con la seguridad de la información y mejora continua del sistema de gestión de seguridad de la información;

5. **Gestión protección de la privacidad:** Establecer y asignar claramente las autorizaciones, recursos y responsabilidades para la gestión integral de la seguridad y privacidad de la información, definiendo roles específicos con competencias técnicas adecuadas. Implementar procedimientos formales para el manejo de exenciones y excepciones, asegurando su autorización y control conforme a la normativa vigente.

6. **Mejora continua:** Evaluar periódicamente la efectividad de los controles y estrategias implementadas, asegurando su actualización frente a nuevos riesgos y amenazas.

INDICADORES

1. Porcentaje de cumplimiento del plan de seguridad y privacidad de la información
2. Número de incidentes de seguridad de la información detectados, gestionados y mitigados en el período.
3. Porcentaje de personal capacitado en seguridad de la información y sensibilización sobre riesgos