1. NORMATIVA

- **Ley 594 de 2000** – Ley General de Archivo – Criterios de seguridad;
- **Ley 962 de 2005** – Simplificación y Racionalización de Tramite. Atributo de seguridad en la información electrónica de entidades públicas;
- **Ley 1150 de 2007** – Seguridad de la información electrónica en contratación en línea;
- **Ley 1266 de 2008** – Habeas data financiera, y seguridad de datos personales;
- **Ley 1273 de 2008** – Delitos informáticos y protección del bien jurídico tutelado que es la información;
- **Ley 1341 de 2009** – Tecnologías de la información y aplicación de seguridad;
- **Ley 1437 de 2011** – Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo;
- **Ley 1474 de 2011** – Estatuto anticorrupción "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública";
- **Ley 1712 de 2014** – Ley de transparencia y acceso a la información. "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones";
- **Ley 1581 de 2012** – Ley estatutaria de protección de datos personales;
- **Decreto Ley 019 de 2012** – Racionalización de tramites a través de medios electrónicos. Criterio de seguridad;
- **Decreto 2693 de 2012** – Gobierno electrónico;
- **ISO 27001:2005** - Sistemas de gestión de seguridad de la información.

2. ALINEACIÓN CON EL DIRECCIONAMIENTO ESTRATÉGICO

Plataforma estratégica
La Política de seguridad de la información en la Subred Integrada de Servicios de Salud Sur ESE se articula con la visión institucional desde el enfoque "seremos una Subred Integrada de Servicios de salud, consolidada, sostenible, confiable y accesible".

Objetivo Estratégico

- Garantizar el manejo eficiente de los recursos que aporten a la implementación del modelo de atención en red.

3. ENUNCIADO

La Subred Integrada de Servicios de Salud Sur ESE se compromete a mantener la confidencialidad, integridad y disponibilidad de la información a través de la identificación y mitigación de los riesgos a los cuales está expuesta con el objetivo de asegurar la misma y propender por el establecimiento de una cultura de seguridad informática.

4. OBJETIVO DE LA POLÍTICA

Mantener la seguridad informática de la Subred Integrada de Servicios de Salud Sur ESE con el fin de disponer de información confiable, integra y oportuna que facilite la toma de decisiones institucionales.

5. ALCANCE DE LA POLÍTICA

La política cubre, sin excepción, a todos los procesos de la Entidad, dando cumplimiento a los procesos y procedimientos institucionales.

Con competencia de todos los funcionarios y personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

6. DEFINICIONES

- **Activo de información:** Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Subred Sur ESE y, en consecuencia, debe ser protegido.

- **Acuerdo de confidencialidad:** Es un documento en el que los funcionarios y contratistas de la Subred sur ESE o los provistos por terceras partes manifiestan la voluntad de mantener la confidencialidad de la información de la Subred Sur ESE, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

- **Análisis de riesgos de seguridad de la información:** Proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de perdida de confidencialidad, integridad y disponibilidad de la información.

- **Autenticación:** Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

- **Control:** Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legar.

- **Custodio de activo de información:** Es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

- **Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

- **Identificación del riesgo:** Elemento de control que posibilita conocer los eventos potenciales, estén o no bajo el control de la Subred Sur, que ponen en riesgo la confidencialidad, integridad y disponibilidad de los activos de información, estableciendo los agentes generadores, las causas y los efectos de su ocurrencia.

- **Integridad:** Es la protección de la exactitud y estado completo de los activos.

- **Inventario de activos de información:** Es una lista ordenada y documentada de los activos de información pertenecientes a la Subred Sur ESE.

- **Propietario de la información:** Es la unidad organizacional o proceso donde se crean los activos de información.

- **Responsable por el activo de información:** Es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

- **Colaboradores:** Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

- **Vulnerabilidades:** Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Subred Sur ESE (amenazas), las cuales se constituyen en fuente de riesgo.

7. DESARROLLO

La Subred Integrada de Servicios de Salud Sur ESE, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para la Subred Integrada de Servicios de Salud Sur ESE, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica según como se define en el alcance, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema General de Seguridad de la Información estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en funcionarios y personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- Garantizar la continuidad del negocio frente a incidentes.
- La Subred Sur ESE ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

A continuación se establecen 12 principios de seguridad que soportan el Sistema de Gestión de Seguridad de la Información de la Subred Integrada de Servicios de Salud Sur ESE:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios y personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- La Subred Integrada de Servicios de Salud Sur ESE protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

- La Subred Integrada de Servicios de Salud Sur ESE protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- La Subred Integrada de Servicios de Salud Sur ESE protegerá su información de las amenazas originadas por parte del personal.
- La Subred Integrada de Servicios de Salud Sur ESE protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La Subred Integrada de Servicios de Salud Sur ESE controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La Subred Integrada de Servicios de Salud Sur ESE implementará control de acceso a la información, sistemas y recursos de red.
- La Subred Integrada de Servicios de Salud Sur ESE garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La Subred Integrada de Servicios de Salud Sur ESE garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La Subred Integrada de Servicios de Salud Sur ESE garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La Subred Integrada de Servicios de Salud Sur ESE garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

8. NIVELES DE RESPONSABILIDAD SOBRE EL SEGUIMIENTO Y EVALUACIÓN

A partir de las líneas de defensa establecidas dentro del Modelo Integrado de Planeación Y Gestión, se define las siguientes responsabilidades con respecto a la gestión, seguimiento y evaluación:

Primera línea de defensa: Jefe sistemas de Información TICS
Funciones:

- Implementación Política de Seguridad de la información.
- Diligenciamiento autoevaluación en el marco del Modelo Integrado de Planeación y Gestión

Segunda línea de defensa: Oficina Asesora de Desarrollo Institucional.
Funciones: Verificar el cumplimiento de la política dentro de los procesos responsables.

Tercera línea de defensa: Control Interno
Funciones:

- Control preventivo y detectivo.
- Acompañamiento y asesoría a la primera y segunda línea de defensa.
- Recomendar mejoras en la implementación de la política.

9. INDICADORES

OBJETIVO QUE SE DESEA ALCANZAR CON EL CUMPLIMIENTO DE LA POLÍTICA	METAS PARA DAR CUMPLIMIENTO AL OBJETIVO ESPECÍFICO DE LA POLÍTICA	INDICADOR DE EVALUACIÓN		
		NOMBRE DEL INDICADOR	FÓRMULA	PERIODICIDAD DE MEDICIÓN
Establecer los controles de seguridad de los activos de información de la Subred Integrada de Servicios de	El 100% de los activos de información contaran con	Cumplimiento de la construcción del inventario de activos de información.	Número de procesos inventariados / Número total de	Semestral

Salud Sur ESE.	controles de seguridad.		procesos de la Subred Sur ESE	
Mitigar los riesgos a los que se encuentran expuestos los activos de información y los recursos Físicos informáticos de la Subred Sur ESE, que impidan el logro de los objetivos del SGSI.	El 100% de los riesgos identificados con acciones a mitigar.	Proporción de vigilancia de eventos adversos.	Número total de riesgos materializados / Número total de riesgos identificados y/o priorizados	Mensual
Capacitar a los directivos, funcionarios, contratistas y terceros que laboren o tengan relación con la Subred Integrada de Servicios de Salud Sur ESE, de las políticas, normas y mecanismos que deben cumplir para proteger los activos de información.	Capacitar al 60% del personal que tenga relación con la Subred Sur ESE acerca de seguridad de la información.	Cumplimiento del plan de inducción y reinducción institucional de Seguridad de la información.	Número total de colaboradores capacitados / Número total de colaboradores de la Subred Sur ESE	Semestral

10. PUNTO DE CONTROL

Oficina sistemas de Información TICS.

11. RESPONSABLE

El responsable de realizar actualización y/o modificaciones necesarias a la política es el Jefe de Oficina Sistemas de Información TICS

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrea Fernanda Baró Moreno	Nombre: Jhon Alexander Cepeda Zafra	Nombre: John Jairo Vasquez Herrera	Nombre:Gloria Libia Polania Aguillon
Cargo: Apoyo Administrativo	Cargo: Jefe Oficina Sistemas de Información TICS	Cargo: Referente Direccionamiento Estratégico	Cargo: Gerente (e)
Fecha: 05/11/2019	Fecha: /11/2019	Fecha: 05/11/2019	Fecha:05/11/2019
Firma:	Firma:	Firma:	Firma: