| 1. NOMBRE DE LA POLITICA | POLITICA DE SEGURIDAD DE LA INFORMACION | |
|---|---|---|
| 1.1 Normatividad que soporta la Política | • Ley 594 de 2000 – Ley General de Archivos – Criterios de Seguridad;<br>• Ley 962 de 2005 – Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas;<br>• Ley 1150 de 2007 – Seguridad de la información electrónica en contratación en línea;<br>• Ley 1266 de 2008 – Habeas data financiera, y seguridad en datos personales;<br>• Ley 1273 de 2008 – Delitos Informáticos y protección del bien jurídico tutelado que es la información;<br>• Ley 1341 de 2009 – Tecnologías de la Información y aplicación de seguridad;<br>• Ley 1437 de 2011 Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.<br>• 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"<br>• 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"<br>• Ley 1581 de 2012 – Ley estatutaria de Protección de datos personales;<br>• Decreto Ley 019 de 2012 – Racionalización de trámites a través de medios electrónicos. Criterio de seguridad<br>• Decreto 2693 de 2012 – Gobierno electrónico<br>• ISO 27001:2005 Sistemas de gestión de Seguridad en la Información. | |
| 1.2. Alineación con el Direccionamiento Estratégico | 1.2.1 Plataforma Estratégica | La Política de Seguridad de la Información en la Subred Integrada de Servicios de Salud Sur E.S.E se articula con la Visión Institucional desde el enfoque "seremos una Subred Integrada de servicios de Salud, consolidada, sostenible, confiable y accesible". |
| | 1.2.2 Objetivo estratégico al que le apunta | Objetivo Estratégico N° 2: Garantizar el manejo eficiente de los recursos que aporten a la implementación del modelo de atención en red. |
| 2. ENUNCIADO POLITICA | La Subred Integrada de Servicio 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 objeto de asegurar la misma y propender por el establecimiento de una cultura de seguridad informática. | |
| 3. OBJETIVO POLITICA | 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 | |
| 4. DEFINICIONES A TENER EN CUENTA PARA EL ENTENDIMIENTO DE LA POLÍTICA | | |

- **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 los que los funcionarios y contratistas de La Subred Sur ESE o los provistos por terceras partes manifiestan su 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 pérdida 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 legal.
- **Custodio del 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 fuentes de riesgo.

| 5. OBJETIVOS ESPECIFICOS DE LA POLÍTICA | | | | |
|---|---|---|---|---|
| **5.1. Objetivos que se desean alcanzar con el cumplimiento de la política** | **5.2. Metas para dar cumplimiento al objetivo específico de la política** | **5.3. Indicador de Evaluación** | | |
| | | **Nombre del Indicador** | **Fórmula** | **Periodicidad de medición** |

| 5. OBJETIVOS ESPECIFICOS DE LA POLÍTICA | | | | | |
|---|---|---|---|---|---|
| | 5.1. Objetivos que se desean alcanzar con el cumplimiento de la política | 5.2. Metas para dar cumplimiento al objetivo específico de la política | 5.3. Indicador de Evaluación | | |
| | | | Nombre del Indicador | Fórmula | Periodicidad de medición |
| 1 | Establecer los controles de seguridad de los Activos de Información de la Subred Integrada de Servicios de Salud Sur ESE. | El 100% de los activos de información contaran con controles de seguridad. | Cumplimiento de la construcción del Inventario de Activos de Información, | Número de procesos inventariados / Número total de procesos de la Subred Sur ESE | Semestral |
| 2 | 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 de Mitigación. | Proporción de Vigilancia de Eventos Adversos | Número total de riesgos en estado cerrado / Número total de riesgos identificados y/o priorizados | Mensual |
| 3 | 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 100% personal que tenga relación con la subred Sur acerca de seguridad de información. | Cumplimiento del plan de inducción y re-inducción Institucional en Seguridad de la Información. | Número total de Colaboradores capacitados / Número total de colaboradores de la Subred Sur ESE | Semestral |
| | **6. Cargo del responsable de realizar seguimiento y control al cumplimiento de la política** | JEFE OFICINA SISTEMAS DE INFORMACIÓN TIC | | | |

| ELABORÓ | REVISÓ | APROBO |
|---|---|---|
| **Nombre:** JOSÉ ANTONIO SÁENZ GONZÁLEZ | **Nombre:** JHON ALEXANDER CEPEDA ZAFRA | **Nombre:** CLAUDIA HELENA PRIETO VANEGAS |
| **Firma:** | **Firma:** | **Firma:** |
| **Cargo:** Profesional Gestión TIC | **Cargo:** Jefe Oficina Sistemas De Información Tic | **Cargo:** GERENTE |
| **Fecha: JULIO 2017** | **Fecha: JULIO 2017** | **Fecha: JULIO 2017** |