1. NORMATIVA

- **Constitución Política de 1991 – arts. 15, 20 y 269**

  Art. 15 reconoce el derecho a la intimidad y al hábeas data, base de toda regulación de protección de datos personales.
  Art. 20 garantiza la libertad de informar y recibir información veraz e imparcial.
  Art. 269 ordena que todas las entidades públicas diseñen y apliquen sistemas de control interno, fundamento constitucional del SGSI y del modelo de tres líneas de defensa.

- **Objetivos de Desarrollo Sostenible ODS:**

  ODS 8 Trabajo decente y crecimiento económico, Promueve el empleo digno, la protección laboral y el aumento de la productividad institucional. En el sector público, la transparencia y la eficiencia administrativa son condiciones clave para generar confianza y crecimiento económico sostenible.
  ODS 9 Industria, innovación e infraestructura, Fomenta el empleo digno, la inclusión laboral y la productividad en condiciones de equidad. Una gestión pública transparente y libre de corrupción impulsa un entorno institucional confiable para el desarrollo económico y el bienestar laboral.
  ODS 16 Paz, justicia e instituciones sólidas, Impulsa la construcción de instituciones eficaces, responsables y transparentes, con pleno respeto al Estado de derecho. Este objetivo sustenta las políticas de lucha contra la corrupción, acceso a la información y participación ciudadana como pilares de la gobernanza democrática.

- **Ley 2033 de 2020:** Esta ley establece disposiciones adicionales relacionadas con la ciberseguridad y la protección de datos, incluyendo la creación del Sistema Nacional de Ciberseguridad y la Comisión Intersectorial de Ciberseguridad.
- **Ley 1978 de 2019** "Modernización TIC" Reforma la Ley 1341/2009: unifica y simplifica la institucionalidad del sector TIC, incentiva inversión privada y fija metas de cierre de brecha digital y despliegue de infraestructura. Es el marco más reciente para planes de conectividad y servicios digitales seguros.
- **Ley 1955 de 2019:** Esta ley establece disposiciones relacionadas con la ciberseguridad y la protección de infraestructuras críticas en Colombia. Define las obligaciones y responsabilidades de las entidades encargadas de operar infraestructuras críticas y busca fortalecer la seguridad en línea.
- **Ley 1952 de 2019 –** "Código General Disciplinario": Moderniza el régimen disciplinario: tipifica deberes y faltas de los servidores públicos, incluidas conductas sobre custodia, reserva y uso indebido de la información o los sistemas institucionales. Refuerza la corresponsabilidad de todo funcionario en la seguridad digital.
- **Ley 1908 de 2018:** Por medio de la cual se fortalecen la investigación y judicialización de organizaciones criminales, se adoptan medidas para su sujeción a la justicia y se dictan otras disposiciones.
- **Ley 1712 de 2014:** 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.
- **Ley 1474 de 2011:** 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 1341 de 2009:** Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.
- **Ley 1273 de 2009:** Por medio de la cual se modifica el Código Penal, se crea un nuevo Bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- **Ley 1266 de 2008:** Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia,

comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

- **Ley 1150 de 2007:** Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
- **Ley 599 de 2000:** Por la cual se expide el Código Penal, Tipificación de delitos informáticos más allá de la Ley 1273.
- Decreto 1170 de 2015: Por medio del cual se expide el Decreto Reglamentario Único del Sector Administrativo de Información Estadística.
- **Decreto Distrital 479 de 2024:** Decreto Único del Sector Gestión Jurídica Compila y unifica la normativa distrital sobre gestión jurídica y seguridad de la información; facilita la trazabilidad de obligaciones y establece criterios técnicos que deben observar todas las entidades del Distrito en materia de protección de datos y continuidad de sistemas.
- **Decreto 2106 de 2019:** Normas para simplificar, suprimir trámites existentes en la administración pública.
- **Decreto 620 de 2018:** Este decreto reglamenta la Ley 1581 de 2012 y establece los requisitos específicos para las políticas de tratamiento de datos personales, incluyendo la designación de un encargado de protección de datos y la notificación de brechas de seguridad de datos.
- **Decreto 1170 de 2015:** Comisión Nacional Digital y de Información Estatal Hace parte del Decreto Único del Sector Información Estadística; crea la Comisión Nacional Digital e Información Estatal, responsable de coordinar políticas de información pública y de orientar al Grupo de Respuesta a Emergencias Cibernéticas de Colombia (COLCERT). Sustenta la articulación interinstitucional en ciberseguridad.
- **Decreto 1078 de 2015:** Art. 2.2.9.1.2.2 contemplo los instrumentos para implementar la Estrategia de Gobierno en Línea, dentro de los cuales se exige la elaboración por parte de cada entidad un Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETI, un Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Seguridad y Privacidad de la Información.
- **Decreto 212 de 2014:** Por medio del cual se crea el comité de Gobierno en línea, Anti trámites y Eficiencia Administrativa.
- **Decreto Nacional 2573 de 2014:** Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea, se reglamenta parcialmente la ley 1341 de 2009 y se dictan otras disposiciones.
- **Decreto 2693 de 2012:** Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.
- **Decreto Ley 019 de 2012:** Racionalización de tramites a través de medios electrónicos. Criterio de seguridad.
- **Acuerdo Distrital 927 de 2024: Plan Distrital de Desarrollo "Bogotá Camina Segura 2024-2027"** Establece las líneas estratégicas, programas y metas del Distrito, incluyendo compromisos de transformación digital, gobierno abierto y servicios seguros. La política de seguridad debe alinearse con sus metas para evitar inconsistencias regulatorias.
- **Acuerdo 03 de 2015 del AGN:** Por el cual se establecen los lineamientos generales para las Entidades del Estado en cuanto a la gestión de documentos electrónicos generado como resultado del uso de medios tecnológicos de conformidad con lo establecido en el Capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el Decreto 2609 de 2012

- **Compes 3854 de 2106:** Política Nacional de Seguridad Digital.

- **Resolución 500 de 2021** - Lineamientos y estándares para la estrategia de Seguridad Digital.

- **ISO 27001:2013:** Sistemas de gestión de seguridad de la información.

2. ALINEACIÓN CON EL DIRECCIONAMIENTO ESTRATÉGICO

La Política de seguridad digital de la Subred integrada de Servicios de Salud Sur ESE se articula con la Plataforma Estratégica desde el enfoque:

Misión: La Subred Integrada de Servicios de Salud Sur E.S.E., brinda a través de un Modelo basado en la Atención Primaria Social, integral e integrado, servicios de salud enfocados a una gestión de riesgo, con excelencia, humanizada y comprometida con MÁS SALUD Y MÁS BIENESTAR; contando con un talento humano altamente calificado, transparente, comprometido, con vocación de docencia y servicio soportado en una gestión del conocimiento, innovadora e investigativa que contribuye al mejoramiento de las condiciones de vida de la población urbana y rural bajo un enfoque diferencial.

Visión: Consolidarnos en el año 2028, como una Empresa Social del Estado referente a nivel nacional en la Prestación de Servicios de Salud con MÁS Bienestar, con estándares superiores de calidad, líderes en docencia, con avances significativos en investigación, sostenibilidad financiera y ambiental; manteniendo un enfoque incluyente, diferencial y multicultural que promueva la intersectorialidad aportando al mejoramiento de la calidad de vida de nuestros usuarios, familias y comunidad urbana y rural.

Objetivo Estratégico

Estratégico Nro. 3: Enfoque a la Gestión y Desempeño – SOGC – Procesos y Procedimiento – Innovación – Tecnología – Sistemas De Información justificación: Esta política permite proteger los sistemas de información, los datos personales y la infraestructura tecnológica que soportan los procesos administrativos y asistenciales. Al implementar controles de ciberseguridad, gestión de accesos, respaldo de información y medidas contra incidentes digitales, se garantiza la continuidad operativa, la confianza institucional y la integridad de los servicios prestados, aspectos esenciales para un soporte institucional robusto, seguro y alineado con la transformación digital del sector salud.

Valor Asociado

Responsabilidad: Entendido como el compromiso de actuar con diligencia, rigor y conciencia institucional en el uso, protección y gestión de la información digital. La responsabilidad de cada servidor público frente a los activos tecnológicos y los datos institucionales es clave para garantizar la seguridad, la continuidad de los servicios y la confianza de la ciudadanía en los sistemas de salud. Este valor impulsa una cultura organizacional que previene incidentes, protege los derechos de los titulares de la información y asegura la trazabilidad institucional.

3. ENUNCIADO

La Subred integrada de Servicios de Salud Sur ESE, se compromete a diseñar estrategias para mejorar las capacidades en materia de seguridad digital al interior de la entidad, por medio de la definición de roles y responsabilidades en seguridad digital, que permitan generar confianza y adaptación para el futuro digital, acorde con las necesidades de los diferentes grupos de valor.

4. OBJETIVO DE LA POLÍTICA

Diseñar estrategias que conlleven a mejorar las capacidades institucionales para la identificación, gestión, tratamiento, mitigación de los riesgos de seguridad digital y proteger la información, sistemas informáticos y las redes de una organización contra amenazas y riesgos cibernéticos.; generando confianza digital y adaptación para el futuro digital.

5. ALCANCE DE LA POLÍTICA

La política cubre, sin excepción, a todos los procesos de la entidad, con competencia de todos los colaboradores, personas Naturales o Jurídicas, proveedores que provean servicios o productos a la entidad.

6. DEFINICIONES

- **Activo de Información:** Es todo aquello que en la entidad es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **Amenaza:** Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Copias de respaldo:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **Dato**: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Gestión de riesgos de seguridad digital:** es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **Grupos de Valor**: Medición estadística, mediante la cual se pueden clasificar y asociar conjuntos de personas con características similares. La Subred Integrada de Servicios de Salud Sur, en su Documento de caracterización de grupos de valor DI-DE-OD-03-V1, identifica las características, demográficas, geográficas, necesidades, intereses, preferencias, expectativas y motivaciones de los grupos de valor identificados y clasificados en seis (6) Grupos de Valor. (Colaboradores, Usuario Familia y Comunidad, Proveedores y Servicios Tercerizados, Gobierno, Medio Ambiente, Educación y Formación).
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Información:** Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **MSPI**: Modelo de Seguridad y Privacidad de la Información.
- **Resiliencia:** Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (Documento CONPES 3854).
- **Responsabilidad:** Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales.
- **Riesgo:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.
- **Riesgo de seguridad digital:** Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **Vulnerabilidad**: Es una debilidad del sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **Entorno digital:** Ambiente, tanto físico como virtual sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías

web.

- **Incidente digital:** evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el entorno digital y que genera impactos sobre los objetivos.

7. DESARROLLO

La Subred Integrada de Servicios de Salud Sur E.S.E., en concordancia con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Gobierno Digital, y la normativa nacional en materia de protección de la información, adopta la presente política con el fin de asegurar la confidencialidad, integridad, disponibilidad, trazabilidad y resiliencia de la información institucional.

Esta política articula el Sistema de Gestión de Seguridad de la Información (SGSI) con los planes estratégicos de tecnología (PETI), el sistema de control interno, la gestión documental y la continuidad del negocio, incluyendo a todos los actores: funcionarios, contratistas, proveedores y ciudadanía.

1. Enfoque institucional de gestión del riesgo digital

La Subred implementará un enfoque basado en riesgo para la protección de activos digitales, bajo la metodología de gestión de riesgos establecida en el MIPG y los estándares ISO 31000 e ISO 27005. El análisis de riesgos será sistemático, documentado y actualizado periódicamente, e incluirá una categorización por impacto y probabilidad sobre los sistemas de información críticos. Los planes de tratamiento serán parte integral y actualizable del Plan de Seguridad y Privacidad de la Información (PSPI), articulados al PETI y validados por el Comité Institucional de Gestión y Desempeño. Esto permitirá tomar decisiones oportunas en materia de mitigación y priorización de inversiones.

2. Principios rectores de la política

Principio	Alcance	Acción mínima esperada
Seguridad digital	Cumplimiento del SGSI y sus controles. Establece el marco para el uso responsable de los activos digitales, protocolos de seguridad, políticas de uso aceptable y respuesta ante incidentes.	Uso aceptable, cumplimiento de normas, participación en jornadas de sensibilización, reporte inmediato de incidentes.
Confianza del usuario	Calidad y oportunidad de la información. La seguridad debe garantizar que la información sea veraz, accesible cuando se requiera y que mantenga su integridad durante todo su ciclo de vida.	Reportar fallas en integridad o accesos indebidos en menos de 24 horas. Aplicar protocolos de recuperación.
Innovación tecnológica	Adopción de soluciones "por diseño seguro". Todo nuevo desarrollo tecnológico institucional (software, plataformas, aplicaciones) deberá cumplir requisitos de seguridad desde su concepción.	Evaluación de seguridad en nuevas plataformas o servicios digitales. Incluir revisiones técnicas en todo proyecto TIC.

Protección de activos	Hardware, software, datos e infraestructura tecnológica. Incluye la gestión de inventarios, clasificación de información, monitoreo de accesos, y mecanismos de respaldo físico y lógico.	Clasificación y tratamiento según políticas de datos personales y manuales del SGSI. Sensibilización del personal.
Cultura de seguridad	Formación, ética y responsabilidad individual e institucional. La gestión de la seguridad requiere compromiso colectivo, liderazgo visible, campañas pedagógicas y generación de alertas tempranas.	Capacitación obligatoria anual para todo el personal. Campañas internas de buenas prácticas digitales.

3. Articulación con componentes del MIPG y el Gobierno Digital

- Integración con el Modelo de Gobierno Digital (MinTIC), especialmente en lo relacionado con arquitectura TI, interoperabilidad, servicios digitales seguros, analítica institucional y protección de datos personales.
- Adopción de lineamientos del Marco de Referencia de Arquitectura Empresarial del Estado y la Resolución MinTIC 500 de 2021, incorporando requisitos técnicos y organizacionales de seguridad digital.
- Alineación con los instrumentos del MIPG: PEI, POAI, políticas institucionales, y planes de acción. El SGSI se documentará en el sistema de gestión institucional y se auditará conforme al cronograma de la Oficina de Control Interno.
- Inclusión del componente de seguridad digital como línea estratégica en el Plan Estratégico de Tecnología de la Información (PETI), asegurando la asignación de recursos y responsabilidades.

4. Integración con el Sistema de Control Interno y Gestión Documental

- La Oficina de Control Interno ejercerá la tercera línea de defensa, auditando la eficacia del SGSI y verificando la trazabilidad de la información en todas las fases de su ciclo de vida.
- El SGSI adoptará los lineamientos del Archivo General de la Nación (Acuerdo 03 de 2015) para asegurar que la evidencia digital conserve validez jurídica y técnica.
- Toda evidencia de la operación de controles (registros de accesos, bitácoras de respaldo, actas de incidentes) se archivará conforme al Cuadro de Clasificación Documental y los tiempos de retención vigentes.

Los mecanismos de archivo estarán alineados con el Sistema Integrado de Conservación Documental y se verificará periódicamente su consistencia a través de auditorías internas.

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:

Línea Estratégica: A cargo de la Gerencia, define el Marco General de la Política y supervisa su cumplimiento.

Primera línea de defensa: Jefe sistemas de información TICS, su rol principal es divulgar e implementar la política de Seguridad Digital, realizar seguimiento a las acciones definidas desde el autocontrol, además del diligenciamiento de la autoevaluación en el marco del Modelo Integrado de Planeación y Gestión.

Segunda línea de defensa: Oficina Asesora de Desarrollo institucional, su rol principal es realizar el monitoreo a la implementación de la política, medición de indicadores, evaluar la implementación de las estrategias y gestión de la primera línea.

Tercera línea de defensa: A cargo de la Oficina de Control Interno, quien provee una evaluación objetiva y de aseguramiento a la entidad a través del proceso de auditoría interna sobre la efectividad de las políticas, su implementación y la adecuada operación del Sistema de Control Interno.

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
Monitorear y evaluar la eficacia de los controles priorizados en la Matriz de Riesgos de Seguridad de la Información de la Subred Integrada, de Servicios de Salud Sur ESE.	Ejecutar de forma semestral el ciclo de seguimiento en la plataforma Almera: registrar métricas de cada control, validar evidencias y generar planes de mejora para las brechas detectadas.	Porcentaje de monitoreo de controles definidos en la matriz de seguridad de la información	(Número de controles Monitoreados / Número de controles definidos) x 100	Semestral
Fortalecer la cultura de seguridad digital e informática de los usuarios en los procesos administrativos mediante simulaciones periódicas que pongan a prueba y mejoren los controles institucionales.	Planificar y ejecutar simulaciones de ciberseguridad cada seis meses, evaluar la eficacia de los controles, documentar resultados y aplicar acciones de mejora derivadas de los hallazgos.	Realizar simulaciones programadas de Ciberseguridad	(Número de cantidad de simulaciones realizadas / total de simulaciones programadas) x 100	Anual

10. PUNTO DE CONTROL

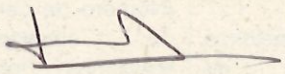
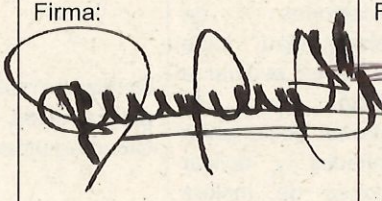
- Como Punto de Control de la Política de Seguridad Digital, la Oficina TIC debe, al cierre de cada semestre, revisar en la plataforma Almera el avance del Plan de Tratamiento de Seguridad Digital, registrar el cumplimiento de los indicadores de seguridad definidos para el proceso y contrastar estos resultados con la Matriz de Riesgos Institucional vigente para confirmar que los controles priorizados siguen siendo pertinentes.
- El informe resultante que consolidará el porcentaje de controles monitoreados, el estado de las acciones correctivas y las simulaciones garantizando así el seguimiento por la segunda y tercera línea de defensa y cerrando el ciclo de mejora continua del SGSI.
- Se realizará dentro de los primeros 15 días de los meses de julio y enero, reportando a la Segunda línea de defensa por el medio que se convenga.

11. RESPONSABLE

Jefe de Oficina Sistemas de información TICS.

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO
1	06/08/2021	Creación del documento Política de Seguridad Digital.
2	19/10/2023	Articulación con la Plataforma estratégica 2020-2024-lineamientos MIPG, desarrollo, indicadores, puntos de control.
3	20/10/2025	Ajuste a normatividad, desarrollo, punto de control. Articulación con la Plataforma Estratégica Institucional 2024-2028.

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Andrés Felipe Cubillos García	Nombre: Julio Andrés Sánchez Sánchez	Nombre: Fredy Orlando Corredor Camargo	Nombre: Viviana Marcela Clavijo
Cargo: Profesional especializado Seguridad informática e Información.	Cargo: Jefe Oficina Sistemas de Información TIC	Cargo: Jefe Oficina Asesora de Desarrollo Institucional	Cargo: Gerente
Fecha: 10/06/2025	Fecha: 20/10/2025	Fecha: 05/11/2025	Fecha: 05/11/2025
Firma: 	Firma: 	Firma: 	Firma: