1. NORMATIVA

- **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
- **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 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 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 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.
- **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 212 de 2014:** Por medio del cual se crea el comité de Gobierno en línea, Anti trámites y Eficiencia Administrativa.
- **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 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.
- **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 2106 de 2019:** Normas para simplificar, suprimir trámites existentes en la administración pública.
- **ISO 27001:2013:** Sistemas de gestión de seguridad de la información.
- **Compes 3854 de 2106:** Política Nacional de Seguridad Digital.
- **Resolución 500 de 2021** - Lineamientos y estándares para la estrategia de Seguridad Digital.

2. ALINEACIÓN CON EL DIRECCIONAMIENTO ESTRATÉGICO

Plataforma estratégica

La Política de seguridad digital 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 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 protección de la información, disminuyendo el impacto generado sobre sus activos; 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

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 digitales 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 valor 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 digital estarán determinadas por las siguientes premisas:

- Cumplir con los principios de seguridad digital.
- Mantener la confianza de sus usuarios con relación a la información.
- Apoyar la innovación tecnológica,
- Proteger los activos tecnológicos.
- Establecer los procedimientos e instructivos en materia de seguridad digital.
- Fortalecer la cultura de seguridad digital en funcionarios y personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.
- Responder la continuidad del negocio frente a incidentes presentados.
- El correo electrónico, claves de internet, y chat son de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de estas y de sus contraseñas, por ningún motivo se debe permitir a otra persona acceder a estos recursos.
- La Entidad deberá restringir el acceso a los sitios relacionados con redes sociales, con el fin de aumentar la velocidad de acceso y el riesgo de virus. Si algún Colaborador por motivos de trabajo requiere acceso a ellos, deberá enviar la solicitud a la Oficina de Sistemas de Información Tic.
- Toda información que se publique o divulgue por cualquier medio de internet de cualquier colaborador que sea creado a nombre personal como redes sociales, se considera fuera del dominio de la Subred Integrada de Servicios de Salud Sur E.S.E, por lo tanto, su integridad, confiabilidad, disponibilidad y daños y perjuicios que se puedan generar, serán de completa responsabilidad de la persona que las haya generado.
- Los equipos de cómputo y de comunicaciones de la Entidad deben utilizarse únicamente para asuntos

de carácter institucional.

- El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la Subred Integrada de Servicos de Salud E.S.E y deben ser usados únicamente para el cumplimiento de la misión de la Entidad.
- Los usuarios deben tratar los mensajes de correo electrónico, chat y archivos adjuntos como información de propiedad de la Subred Integrada de Servicos de Salud E.S.E. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones.
- Cuando un colaborador que tiene asignada una cuenta de correo de la entidad, deberá entregar a la Subred Integrada de Servicos de Salud E.S.E. los usuarios y password asignados, de igual manera dicha información debe entregarse cuando exista un proceso de empalme.

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
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.	Porcentaje de inventario de activos de información con controles de seguridad. .	Numero de procesos institucionales con activos de información inventariados y con controles de seguridad en el periodo / Total de procesos institucionales programados en el mismo período *100	Semestral
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.	Monitorear el 100% de los riesgos digitales identificados con acciones a mitigar.	Porcentaje de riesgos digitales con seguimiento.	Número total de riesgos digitales con seguimiento y materializados en el periodo / Total de riesgos digitales identificados en	Semestral

			el mismo periodo * 100	
Capacitar a los Directivos, Colaboradores y proveedores que laboren o tengan relación con la Subred Integrada de Servicios de Salud Sur ESE, en temas de seguridad digital.	Lograr un cumplimiento mayor o igual al 70% el Plan de Inducción institucional de Seguridad Digital	Cumplimiento del plan de inducción y reinducción institucional de Seguridad Digital.	Numero de inducciones ejecutadas del plan de inducción y reinducción institucional de seguridad digital en el periodo / Total de inducciones programas del plan de inducción y reinducción de seguridad digital. *100	Anual

10. PUNTO DE CONTROL

Plan de Tratamiento de Seguridad Digital.
Indicadores del Plan Operativo del Proceso.
Matriz de Riegos Institucional.
Seguimiento trimestral.

11. RESPONSABLE

Jefe de Oficina Sistemas de información TICS.

12. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DEL CAMBIO

ELABORADO POR	REVISADO POR	CONVALIDADO	APROBADO
Nombre: Diana Carolina Ussa Ruiz	Nombre: Diana Carolina Ussa Ruiz	Nombre: Gloria Libia Polania Aguillón	Nombre: Luis Fernando Pineda Ávila
Cargo: Jefe Oficina Sistemas de Información TICS	Cargo: Jefe Oficina Sistemas de Información TICS	Cargo: Referente Direccionamiento Estratégico	Cargo: Gerente
Fecha: 27/07/2021	Fecha:27/07/2021	Fecha: 06/08/2021	Fecha: 06/08/2021
Firma:	Firma:	Firma:	Firma: