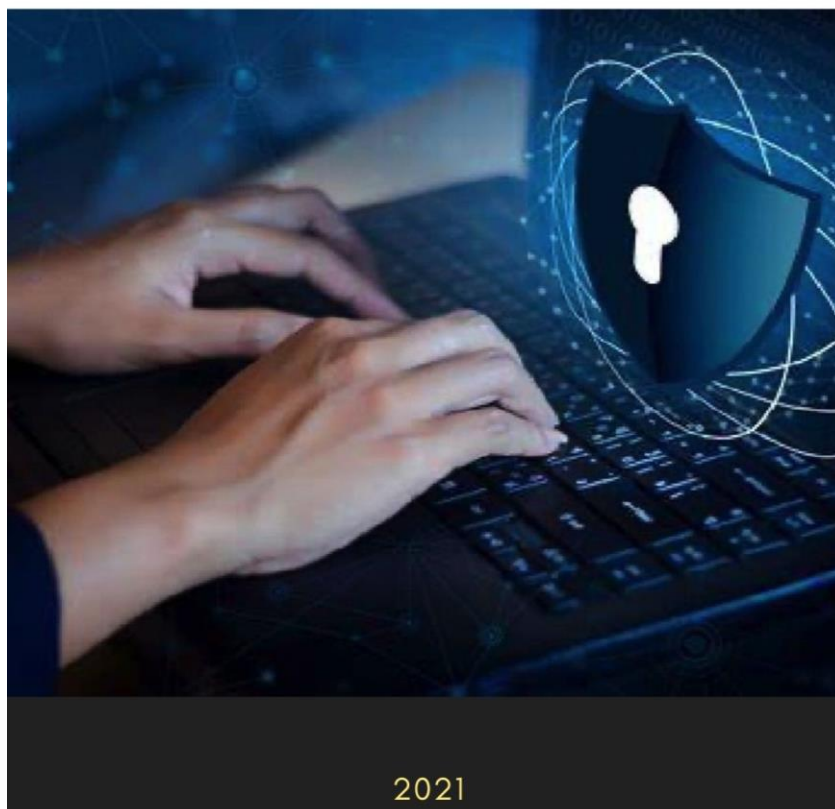


 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 1 DE 17
		FECHA: 21/10/2021

**SUBRED INTEGRADA DE SERVICIOS DE
SALUD NORTE E.S.E**

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 2 DE 17
		FECHA: 21/10/2021

CONTENIDO

1.	JUSTIFICACIÓN	4
2.	OBJETIVO GENERAL.....	4
3.	ALCANCE Y CAMPO DE APLICACIÓN.....	4
4.	ENFOQUE DIFERENCIAL	4
5.	MARCO CONCEPTUAL.....	5
5.1.	Marco legal	5
5.2.	Marco teórico	5
5.2.1.	Glosario	5
6.	DESARROLLO DEL CONTENIDO.....	6
6.1.	Talento humano	6
6.2.	Equipos biomédicos	7
6.3.	Dispositivos médicos e insumos requeridos	7
6.4.	Descripción de las actividades	7
6.4.1.	Política de Seguridad y privacidad de la Información de la Subred Integrada de Servicios de Salud Norte ESE.	7
6.5.	Políticas de Seguridad de la información.....	7
6.5.1.	Política Dispositivos Móviles	7
6.5.2.	Política de Teletrabajo.	8
6.5.3.	Política de Seguridad de los Recursos Humanos	8
6.5.4.	Política de Gestión de Activos.	8
6.5.5.	Políticas Control de Acceso.....	8
6.5.6.	Políticas Seguridad Física y del Entorno	9
6.5.7.	Políticas Seguridad en las Operaciones.....	9
6.5.8.	Políticas Seguridad de las Comunicaciones	9
6.5.9.	Políticas de Relaciones con los Proveedores	9
6.5.10.	Políticas de Gestión de Incidentes de Seguridad	10
6.5.11.	Política de uso de Activos de Información.....	10
6.5.12.	Políticas de seguridad del centro de datos y centros de cableado	10
6.5.13.	Política de seguridad de los equipos	11
6.5.14.	Política de gestión de vulnerabilidades	12

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 3 DE 17
		FECHA: 21/10/2021

6.5.15.	Política de Transferencia de Información	12
6.5.16.	Política del tratamiento y transferencia de datos	12
6.5.17.	Política de uso adecuado del Internet	15
7.	BIBLIOGRAFÍA	16
	ANEXOS	17

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 4 DE 17
		FECHA: 21/10/2021

1. JUSTIFICACIÓN

El proceso de sistemas de información – TIC de la Subred Norte ESE, determina la información como un activo de alta importancia que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad de la información.

Por tal motivo, el presente manual describe las políticas de seguridad de la información y para la elaboración del mismo, se toma como base las recomendaciones de la Norma ISO 27001:2013, los lineamientos de la estrategia de Gobierno Digital y la directriz de Arquitectura Empresarial del Ministerio de la Tecnología y Comunicaciones MinTic en especial las guías suministradas.

2. OBJETIVO GENERAL

Establecer las Políticas que regulan la Seguridad de la Información, uso de mejores prácticas para el mejoramiento de la disponibilidad, integridad y confiabilidad de la información de la Subred Norte ESE, presentando en forma clara y coherente los elementos que la conforman, los cuales se deben conocer, acatar y cumplir por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred, este se encuentra a cargo de la oficina de Información - TIC.

3. ALCANCE Y CAMPO DE APLICACIÓN

El presente manual de Políticas de Seguridad, aplica a la información de la entidad, sus recursos, procesos y a la totalidad de las actividades que se desarrollan para el alcance de los objetivos de la Subred Integrada de Servicios de Salud Norte E.S.E.

Las políticas contenidas en el presente manual son de obligatorio cumplimiento para todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred Norte ESE, para el adecuado cumplimiento de sus obligaciones y de esta manera lograr un adecuado nivel de protección relacionados con calidad y seguridad de la información.

4. ENFOQUE DIFERENCIAL

No aplica

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 5 DE 17
		FECHA: 21/10/2021

5. MARCO CONCEPTUAL

5.1. Marco legal

NORMA	REGLAMENTACIÓN
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 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.
Norma NTC-ISO/IEC: 27001 - 2013	Estándar internacional para un sistema de gestión de seguridad de la información.
Decreto 103 de 2015	El cual reglamenta parcialmente la ley 1712 de 2014 "Ley de Transparencia "
Ley 1581 de 2012	Reglamenta parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, "Protección de datos personales".
Decreto único reglamentario 1078 de 2015	MinTic – Modelo de Seguridad y Privacidad de Información
Ley 1221 del 2008	Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Decreto 886 de 2014	Por el cual se reglamenta el Registro Nacional de Bases de Datos.
Resolución 512 de 2019	Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información.
CONPES 3701 de 2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.
CONPES 3854 de 2016.	Política Nacional de Seguridad digital.
RESOLUCIÓN NÚMERO 00500 DE MARZO 10 DE 2021"	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
ANEXO 1 MSPI - MINTIC	Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías de la Información y las Comunicaciones FEBRERO 2021

5.2. Marco teórico

5.2.1. Glosario

Teniendo en cuenta lo descrito en (ISO/IEC, 2013), a continuación, se describen las definiciones relacionadas con Seguridad de la Información de acuerdo con la ISO 27001.

- **Acción correctiva:** está definida como cualquier acción que tiene como finalidad la de eliminar una no conformidad y evitar que vuelva a suceder

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 6 DE 17
		FECHA: 21/10/2021

- **Acción preventiva:** Medida a prevenir no conformidades.
- **Aceptación del riesgo:** decisión tomada de asumir el riesgo
- **Activo:** en relación con seguridad de la información, es cualquier elemento relacionado con la información (sistemas, soportes, edificios, personas...) que representen un valor para la entidad.
- **Amenaza:** incidente que puede llegar a causar daño a un sistema o a la organización.
- **Análisis de riesgo:** comprensión de la naturaleza del riesgo y determinar su nivel.
- **Autenticidad:** propiedad que tiene una organización de afirmar lo que es.
- **Confidencialidad:** propiedad de la información para no ser revelada a individuos, empresa o procesos.
- **Control:** son las políticas, los procedimientos, las prácticas y las estructuras organizativas que tienen como finalidad mantener un riesgo en un nivel bajo
- **Inventario de activos:** lista de recursos que incluye hardware, software, documentos, servicios, personas, intangibles, que tiene valor para la empresa y requieren ser protegidos de posibles riesgos.
- **Modelo de Seguridad y Privacidad de la Información MSPI:** Es una herramienta creada por el Ministerio de Tecnologías de la Información y las Comunicaciones MINTIC, con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y Privacidad de la Información.
- **No-Repudio:** No se puede negar un evento o una transacción.
- **Plan de continuidad del negocio:** permite la continuar las operaciones de la empresa en caso de imprevistos que la pongan en peligro.
- **Plan de tratamiento de riesgos:** acciones encaminadas a la gestión de riesgos de seguridad de la información inaceptables y la implementación de las medidas de control para su protección
- **Política:** Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** También llamada protección de datos es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros
- **Seguridad de la información:** confidencialidad, integridad, y disponibilidad de la información.
- **Sistema de Gestión de Seguridad de la Información SGSI:** según (ISO/IEC, 2017), es el conjunto de elementos estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos, cuya finalidad es la de establecer políticas y objetivos de seguridad de la información, basados en enfoque de gestión y mejora continua.
- **Tratamiento del riesgo:** modificar un riesgo a treves de controles.
- **Vulnerabilidad:** debilidad de un activo que se ve aumentada por una o varias amenazas.

6. DESARROLLO DEL CONTENIDO

6.1. Talento humano

Todos los colaboradores de la oficina de sistemas de la subred Norte.

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 7 DE 17
		FECHA: 21/10/2021

6.2. Equipos biomédicos

N/A

6.3. Dispositivos médicos e insumos requeridos

N/A

6.4. Descripción de las actividades

6.4.1. Política de Seguridad y privacidad de la Información de la Subred Integrada de Servicios de Salud Norte ESE.

Subred Integrada de Servicios de Salud Norte se compromete a implementar, mantener y mejorar la seguridad y privacidad de la información, mediante una adecuada gestión de activos, riesgos e incidentes de seguridad de la información; con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información y los datos.

La presente política se encuentra alineada al propósito de la Entidad y apoya el cumplimiento de los objetivos estratégicos.

La Subred Integrada de Servicios de Salud Norte en su propósito de dar cumplimiento con la política de seguridad y privacidad de la información establece los siguientes objetivos:

- Sensibilizar y apropiar la gestión adecuada de seguridad y privacidad de la información en los colaboradores, contratistas, terceros, residentes, practicantes y demás partes involucradas en la entidad.
- La Subred Norte ESE, protegerá la información generada, procesada o resguardada por los procesos asociados a la entidad, su infraestructura tecnológica y activos de información, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta misma.

Nivel de cumplimiento: Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento con la presente política.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a seguridad y privacidad de la información se refiere.

6.5. Políticas de Seguridad de la información

6.5.1. Política Dispositivos Móviles

Es responsabilidad del servidor públicos al que se le asignó el dispositivo móvil evitar la instalación de programas desde fuentes desconocidas, evitar el uso de redes inalámbricas públicas, y mantener desactivadas las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 8 DE 17
		FECHA: 21/10/2021

Los servidores públicos y contratistas deben notificar los dispositivos móviles institucionales con sospecha de infección por malware al personal técnico responsable de la Entidad para el proceso de análisis, evaluación y tratamiento.

6.5.2. Política de Teletrabajo.

Toda información gestionada por la Entidad, y que sea accedida remotamente debe ser utilizada solamente para el cumplimiento de las funciones del cargo o de las obligaciones contractuales con esta.

La Entidad establece los requerimientos para autorizar conexiones remotas a la infraestructura tecnológica necesaria para la ejecución de las funciones de los servidores públicos y contratistas de la entidad, garantizando las herramientas y controles para proteger la confidencialidad, integridad y disponibilidad de las conexiones remotas.

6.5.3. Política de Seguridad de los Recursos Humanos

El área que realice la contratación de personal en la Entidad realiza las verificaciones de los antecedentes (procuraduría, contraloría, policía) de los candidatos al cargo, la formación académica, experiencia y demás información que se requiera, de acuerdo a las leyes, reglamentos de la Entidad y ética pertinente.

Todo servidor público y contratista debe recibir inducción y procesos periódicos de sensibilización en seguridad y privacidad de la información en la Entidad.

El incumplimiento o la violación de las políticas de seguridad de la información de la Entidad, por parte de los colaboradores o terceros, se les aplicará lo establecido en el proceso de investigaciones disciplinarias.

6.5.4. Política de Gestión de Activos.

La Entidad establece los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información.

Cada activo de información de la Entidad debe tener un responsable que debe velar por su seguridad. Los propietarios de la información deben garantizar que todos los activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención.

Es responsabilidad del líder de proceso, jefe de área o director, la identificación y reporte de nuevos activos de información, así mismo mantener actualizada la valoración de estos.

Todos los activos de información deben contar con un responsable, que asegure la protección de la información y los datos que son almacenados en cada uno de ellos.

6.5.5. Políticas Control de Acceso

La Subred Norte ESE es la encargada de definir las reglas y procedimientos con el fin de asegurar acceso físico o lógico de forma controlada a la información y a sus sistemas de información.

Los trabajadores de la Subred Norte ESE, tendrán acceso únicamente a la información que sea requerida para la ejecución de sus funciones y actividades. El acceso a los activos de información se sustenta en las necesidades de uso dentro de los procesos y deben ser autorizados por el

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 9 DE 17
		FECHA: 21/10/2021

responsable de los activos de información. Los roles y responsabilidades de los colaboradores deben ser definidas por cada uno de los líderes de los procesos.

El control de acceso se realizará teniendo en cuenta la asignación de privilegios mínimos para el acceso a la información y de acuerdo al perfil asignado al usuario.

6.5.6. Políticas Seguridad Física y del Entorno

La Subred Norte ESE es la encargada de la elaboración e implementación de programa de seguridad física para el acceso a las instalaciones, esto con el fin de fortalecer la confidencialidad, disponibilidad e integridad de la información.

Los funcionarios y contratistas deben portar el carné que los acredite como trabajadores de la Subred Norte ESE en un lugar visible y durante su permanencia en la institución.

Las áreas donde se procese y almacene la información de la Subred Norte ESE y en las que se encuentre infraestructura que soporte los sistemas de información, estas áreas son de acceso restringido.

6.5.7. Políticas Seguridad en las Operaciones

La Subred Norte ESE, es la encargada de la definición de las reglas, encaminadas a asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de Subred, cuya finalidad es la de garantizar la continuidad de los sistemas de TI.

La oficina de Sistemas de Información – TIC, es la responsable del monitoreo, revisión y brindar el soporte oportuno con el fin de garantizar el uso y desempeño de infraestructura de TI que soporta los sistemas de información.

La oficina de Sistemas de Información – TIC, es la responsable de contar con ambientes de pruebas y producción por separado, cuando sea necesario.

6.5.8. Políticas Seguridad de las Comunicaciones

La oficina de Sistemas de Información – TIC, realiza el control de contenido WEB, filtrando el relacionado a páginas para adultos, mensajería instantánea y demás páginas que no sean de uso institucional, mediante el uso de servidor proxy, firewall o control que mejor se ajuste a la necesidad.

La transferencia de información deberá realizarse protegiendo la confidencialidad, integridad y disponibilidad de los datos de acuerdo con la clasificación del activo tipo información involucrada.

6.5.9. Políticas de Relaciones con los Proveedores

La Entidad controla las relaciones con proveedores, y en particular aquellos que tienen acceso a la información. La información está suficientemente protegida con base a los acuerdos y contratos correspondientes. Esta protección debe contemplarse antes, durante y a la finalización del servicio.

Cualquier cambio que se realice con algún proveedor de TI o de los procesos misionales, debe aplicarse mediante el procedimiento de gestión de cambios establecido en la Entidad.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 10 DE 17
		FECHA: 21/10/2021

6.5.10. Políticas de Gestión de Incidentes de Seguridad

La Subred Norte ESE, es la encargada de establecer los procedimientos con el fin de asegurar la comunicación de la ocurrencia de los eventos e incidentes de seguridad presentados a los activos de información, y ser atendidos de forma oportuna y determinar las medidas correctivas requeridas.

Es necesario que los funcionarios y contratistas de la Subred adopten buenas prácticas para el reporte de los eventos e incidentes de seguridad que puedan generar un impacto negativo sobre los activos de información. Se hace necesario tomar las acciones correctivas necesarias y oportunas ante el reporte de estos eventos de seguridad.

Contar con el registro de evidencias relacionadas con el reporte de incidentes de seguridad, con el fin de realizar el seguimiento respectivo y el soporte si es necesario recurrir a entes externos para acciones legales.

La Entidad establece los procedimientos a seguir para el registro y gestión de incidentes de seguridad, con el objeto de implementar herramientas y controles que permitan mitigar su ocurrencia.

6.5.11. Política de uso de Activos de Información

La Subred Norte ESE, implementará los lineamientos y directrices con el fin de lograr y mantener la protección adecuada de los activos de información mediante la asignación de responsables a cargo de acuerdo con sus roles y funciones.

La Subred Integrada de Servicios de Salud Norte ESE como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma. El inventario de los activos de información se realiza con la finalidad de identificar y clasificar de acuerdo a la normatividad vigente, para su posterior administración y uso en las diferentes áreas, enfocadas en los objetivos y estrategias de la entidad.

La administración y operación realizada con los activos de información propiedad de la Subred Norte ESE, debe estar orientada única y exclusivamente a cumplir con los procesos de la empresa. Los activos de propiedad de la Subred, que son asignado a un funcionario o contratista, deben ser entregado al finalizar el vínculo laboral, ya sea por cambio de funciones o finalización del contrato, se debe hacer la entrega de documentos institucionales, equipos de cómputo, dispositivos móviles, periféricos, manuales e información que se encuentre a su cargo y que este en los dispositivos.

6.5.12. Políticas de seguridad del centro de datos y centros de cableado

La Subred Norte ESE, establece los lineamientos para las instalaciones del centro de datos o de los centros de cableado.

Los centros de cómputo, cableado y cuartos técnicos de la Subred Norte ESE, se debe contar con mecanismos para la prevención de amenazas ambientales (temperatura, humedad, fuego, etc.), las cuales las debe especificar el proveedor de los equipos de acuerdo a las normas técnicas.

Los gabinetes deben permanecer cerrados y bajo llave para evitar el ingreso de personal no autorizado, estas llaves deben permanecer bajo custodia de la Oficina de Sistemas de Información – TIC.

Los elementos de propiedad de la Subred, que componen los centros de cómputo y de cableado deben estar clasificados e identificados para su correspondiente registro en el módulo de Activos

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 11 DE 17
		FECHA: 21/10/2021

Fijos del sistema de información institucional. Al mismo los dispositivos en calidad de préstamo o comodato deben registrarse en el módulo de activos fijos sin datos de placa y con la observación correspondiente.

No se debe almacenar, mantener y/o guardar ningún tipo de elemento que no corresponda a la prestación del servicio del centro de cómputo, de igual forma material inflamable dentro de las áreas usadas para el procesamiento o almacenamiento de información, de igual forma las áreas donde se encuentre la infraestructura de TI que soporta los sistemas de información de la Subred.

Para el ingreso a los centros de cómputo se debe diligenciar el formato Control de Acceso Data Center AP-GI-F-55

En los centros de datos o de los centros de cableado, no se tiene permitido:

- Fumar
- Introducir alimentos o bebidas.
- Portar armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipos sin autorización.
- Modificación de la configuración del equipo sin autorización.
- Alterar o dañar etiquetas que contiene la identificación de los sistemas de información.
- Extraer información de los equipos sin autorización.

6.5.13. Política de seguridad de los equipos

La Subred Norte ESE, establece las reglas y procedimientos con el fin de asegurar la protección de la información de los equipos de cómputo.

No se autoriza realizar cambios en la configuración de los equipos, como conexiones de red, usuarios locales, protector de pantalla, entre otros, por parte de los usuarios. Estas modificaciones las realiza únicamente la Oficina de Sistemas de Información – TIC.

Los funcionarios y contratistas deben tener en cuenta:

- Es responsabilidad de los funcionarios y contratistas no afectar el funcionamiento y/o configuraciones existentes sobre los equipos, sin la autorización de la oficina de Sistemas de Información – TIC, se encuentra prohibido fumar, beber y/o consumir cualquier tipo de alimento, de acuerdo al documento AP-GI-I-04-INSTRUCTIVO USO RECURSOS TECNOLÓGICO.
- Cuando se realicen actividades relacionadas con mantenimiento preventivo o correctivo, se hace necesario el registro con el fin de llevar la trazabilidad, involucrados y actividades desarrolladas.
- No se encuentra autorizado el retiro y/o movimientos entre áreas o fuera de la Subred Norte ESE, activos de información sin la autorización del responsable y el registro en los formatos respectivos.
- Todos los equipos que contengan información y que requieran ser reutilizados o su vida útil llega a su fin, se hace necesario el borrado seguro.
- Los funcionarios y contratistas son responsables de mantener la información que está a su cargo.
- En el caso de requerir el traslado de los activos de información entre las sedes de la Subred, se debe diligenciar el formato AP-AT-F-01 Traslado Devolutivos e inventarios.
- La Subred Norte ESE tiene restringida la instalación de software no autorizado, esto lo realiza a través del establecimiento de políticas y el suministro de los permisos a personal autorizado del área de TI.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 12 DE 17
		FECHA: 21/10/2021

6.5.14. Política de gestión de vulnerabilidades

La Subred Norte ESE, es la encargada de realizar un análisis de vulnerabilidades a todos los activos de información, este análisis se debe realizar de forma periódica a toda la infraestructura de TI con el fin de hacer la evaluación de los riesgos y determinar las medidas respectivas para su mitigación. Dichas pruebas se realizarán únicamente con la autorización del jefe de la oficina de sistemas, a treves de un documento controlado en donde se detallen las actividades, tiempo y alcance del mismo.

6.5.15. Política de Transferencia de Información

La Subred Norte ESE, a través de la oficina de Sistemas de Información – TIC, asignara una cuenta de correo a los funcionarios y contratistas, previa solicitud por parte de los líderes de los procesos de la empresa.

La oficina de Sistemas de Información – TIC es la encargada de proporcionar el servicio de correo institucional, vigilar su correcto uso y funcionamiento. Dichos correos tienen un espacio limitado, por lo que los funcionarios y contratistas deben depurarlo continuamente, con el fin de mantener el espacio disponible.

Los funcionarios y contratistas son los responsables de la salvaguardia de la información que se encuentra en su cuenta de correo electrónico, por tal razón la información contenida en el buzón es de carácter privado y se debe manejar como una comunicación directa entre los interesados. De igual forma los usuarios son los responsables de la información enviada desde su cuenta. Los usuarios no deben abrir archivos adjunto cuando sean desconocidos o que este sea de dudosa procedencia. La oficina de sistema de Información – TIC, debe establecer los procedimientos para la cancelación o inactivación de cuentas que demuestren inactividad por un periodo determinado, de sebe tener en cuenta los usuarios que se encuentren en periodo de vacaciones, licencias y que hayan sido reportados con anterioridad.

6.5.16. Política del tratamiento y trasferencia de datos

La Subred Integrada de Servicios de Salud Norte ESE, identificara las fuentes que generan información al interior de la entidad, con el fin de asegurar su confidencialidad, integridad y disponibilidad de los datos personales.

Se identificarán los sistemas de información, repositorios y recursos informáticos que almacenan, recolectan y procesan datos personales, para fines institucionales.

Los usuarios son los responsables del buen uso y manejo de la información que este a su cargo.

Según la ley 1581 del 2012 la Subred Integrada de Servicios de Salud Norte ESE dará cumplimiento a la norma que expresa cuando la información se obtenga, registre, use, transmita y actualice, previa autorización expresa y voluntaria del titular de la información.

Por su parte la Historia Clínica, está regulada por la Ley 23 de 1981 y por la Resolución 1995 de 1999, en cuanto al diligenciamiento, administración, conservación, custodia y confidencialidad de las historias clínicas, conforme a los parámetros del Ministerio de Salud y del Archivo General de la Nación.

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 13 DE 17
		FECHA: 21/10/2021

La Subred Integrada de Servicios de Salud Norte ESE está comprometido para actuar con responsabilidad y proteger la privacidad custodiando la información en bases de datos y archivos físicos.

Datos de menores de edad: El suministro de datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de la familia o representantes legales del menor, en concordancia con la establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia”.

De la Autorización: La Subred Integrada de Servicios de Salud Norte ESE requiere la autorización previa informada y expresa del titular la cual será obtenida por medios escritos bien sea físicos o electrónicos, de tal manera que pueda ser objeto de consulta posterior.

Al solicitar la información el Titular se debe informar de manera clara la finalidad para la cual se recaudan los datos personales, el tratamiento al cual pueden ser sometidos, sus derechos y los medios a través de los cuales puede ejercerlos y la facultad de autorizar o no el tratamiento en caso de datos sensibles.

No se requiere autorización del Titular de los datos personales cuando se trate de:

- Responder a una orden judicial o cuando los solicita una entidad pública o administrativa en ejercicio de sus funciones legales.
- Datos personales de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Información autorizada por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el registro civil de las personas.
- Datos de niños, niñas y adolescentes

Derechos del titular: El Titular tendrá derecho a conocer, rectificar y actualizar sus datos personales, solicitar prueba de la autorización salvo casos excepcionales por ley, ser informado sobre el uso que se les da a sus datos personales, presentar consultas e interponer quejas, solicitar revocatoria a la Subred Integrada de Servicios de Salud Norte ESE por incumplimiento en la normatividad y a acceder de manera gratuita a los datos personales que hayan sido objeto de tratamiento.

Responsable del tratamiento de datos personales: En esta Política se identifica como responsable de los datos personales a:

LA SUBRED INTEGRAL DE SERVICIOS DE SALUD NORTE ESE
NIT 900.971.006-4
Calle 66 No. 15-41 Bogotá D.C., Colombia PBX 57 60 (1) 4431790
www.subrednorte.gov.co

Deberes del responsable: El responsable se compromete a proceder bajo los lineamientos normativos para garantizar en la medida de lo que le corresponde el ejercicio de los derechos de los Titulares de los datos personales, obtenidos en el desarrollo de sus funciones.

Tipo de información registrada: Para facilitar el contacto con los Titulares de la información, se registra y conserva los datos personales o cualquier información vinculada que pueda asociarse a la persona. La Subred Integrada de Servicios de Salud Norte ESE obtiene información a través de las siguientes fuentes.

- Cuando el paciente o usuario voluntariamente brinda información

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 14 DE 17
		FECHA: 21/10/2021

- En los procesos de atención asistencial
- En los procesos de facturación de servicios
- En los procesos de actividades financieros
- En el ejercicio de procesos laborales
- Otras fuentes, que brindan información relacionada con el servicio que el usuario requiere.

La información personal recopilada puede incluir, pero no limitarse a:

- Nombre, direcciones y números de teléfono
- Fecha y lugar de nacimiento, así como su género
- Direcciones de correo electrónico.
- Información necesaria para facilitar el contacto u otros servicios, incluyendo información familiar o laboral.
- Número de cédula, pasaporte, nacionalidad y país de residencia
- Identificación, representación y existencia en caso de personas jurídicas
- Uso de servicios.
- Información personal brindada a través de encuestas u otros métodos de investigación.
- Información personal brindada a la oficina de Atención al Usuario.
- Por la naturaleza de la institución prestadora de servicios de salud, también se registran datos básicos de la persona responsable del paciente, así como la entidad promotora de salud a la que se encuentra afiliado.

Utilización de la información: La Subred Integrada de Servicios de Salud Norte ESE utiliza información personal para contactar a los Titulares a los cuales se les pueda brindar información sobre prestación de servicios de salud, en casos de: divulgación de información científica y actualización tecnológica en la Subred, información sobre campañas de promoción y planes de detección en salud, presentación de convenios para la prestación de servicios de salud con diferentes entidades, información relativa al programa de donación de órganos, información sobre salud pública, entre otras. Además de utilizarla para procesar, confirmar y cumplir con el objeto de funcionamiento de la Subred Integrada de Servicios de Salud Norte ESE o algún otro servicio que el Titular solicite, la subred puede utilizar esta información para fines administrativos y analíticos, tales como administración de sistemas de información, facturación, contabilidad y auditorías, relacionamiento comercial, procesamiento y verificación de medios de pago, correspondencia del área de Atención al Usuario, y/o para el funcionamiento de los programas promocionales que se llagasen a implementar.

La Subred Integrada de Servicios de Salud Norte ESE no vende la información de sus usuarios, ni comparte los datos personales sin autorización del Titular.

La Subred Integrada de Servicios de Salud Norte ESE también usa información de los Titulares para identificar, desarrollar y dar a conocer servicios que a juicio, son valiosos para los usuarios, pacientes y población en general, y puede comunicarse a través del correo electrónico, mensajes de texto o correo físico. En algún momento, podrán recibir información sobre nuevos servicios, habilitación de centros de salud, programas de prevención entre otros.

Durante las reuniones virtuales se debe previamente solicitar autorización a los asistentes para realizar la grabación de la misma, con el fin de cumplir con la normatividad de tratamiento de datos personales, en dado caso que no se reciba observación al respeto, se da por entendida su aprobación.

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 15 DE 17
		FECHA: 21/10/2021

Transferencia y transmisión de datos personales

La Subred Integrada de Servicios de Salud Norte ESE cumple con lo establecido en el artículo 26 de la Ley Estatutaria 1581 de 2012 y se abstiene de transferir datos personales de los Titulares a otros países que no cuenten con iguales o superiores estándares de protección.

Sin embargo, procederán las siguientes excepciones:

Esta prohibición no regirá cuando se trate de:

- a) Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- b) Intercambio de datos de carácter médico, cuando así lo exija el Tratamiento del Titular por razones de salud o higiene pública.
- c) Transferencias necesarias para la ejecución de un contrato entre el Titular y el Responsable del Tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.

Negativa a tratamiento de información: Si el usuario o paciente considera que la Subred Integrada de Servicios de Salud Norte ESE no debe utilizar o compartir su información personal con las finalidades aquí recogidas, o no quiere recibir materiales informativos relativos a la Subred, debe manifestarlo por escrito a la Oficina de Participación Comunitaria y Servicio al Ciudadano de la Subred Integrada de Servicios de Salud Norte ESE a la Calle 66 No. 15-41 Bogotá D.C., Colombia

Cumplimiento de la ley de protección de datos personales: La Subred Integrada de Servicios de Salud Norte ESE asegura la protección de los datos personales de los Titulares adoptando las medidas técnicas, humanas y administrativas necesarias. De igual manera evitará la adulteración, pérdida o uso no autorizado.

Modificaciones y vigencia: La Subred Integrada de Servicios de Salud Norte ESE se reserva el derecho de modificar esta Política en cualquier momento y notificará a los Titulares sobre cualquier cambio, con la actualización del contenido en la página web y en los documentos que la incluyan.

6.5.17. Política de uso adecuado del Internet

Establecer directrices que permitan a los usuarios de la Subred Norte ESE la navegación segura y uso adecuado, con el fin de evitar pérdidas y modificaciones no autorizadas de la información en las aplicaciones de contenido web.

La Subred Norte ESE es consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionara los recursos necesarios para asegurar su disponibilidad y seguridad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias, por tal motivo esta política se aplicara a todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred.

Los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred deben tener en cuenta las siguientes recomendaciones de uso adecuado de internet

 Secretaría de Salud Subred Integrada de Servicios de Salud Norte E.S.E.	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 16 DE 17
		FECHA: 21/10/2021

- La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de la Subred Norte ESE, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso la información.
- La oficina de Sistemas de información-TIC es la encargada de monitorear continuamente el canal o canales del servicio de Internet.
- La oficina de Sistemas de información-TIC debe establecer procedimientos y controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- La oficina de sistemas de información-TIC debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.
- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Subred Norte ESE o que representen peligro para la entidad como: pornografía, terrorismo, hackeo, segregación racial u otras fuentes definidas por la Subred. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización del líder de la oficina de TICS de la Subred Norte ESE.
- La oficina de Sistemas de Información - TIC es la encargada de la autorización de navegación a los usuarios de la Subred Norte ESE, previa solicitud del jefe inmediato.
- La oficina de Sistemas de Información – TIC implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

7. BIBLIOGRAFÍA

El presente Manual de Políticas de Seguridad y Privacidad de la Información se realizó con base con la normatividad vigente y tomando como modelo:

- Manual de Políticas de Seguridad de la Información de la Presidencia de la Republica de Colombia Versión de mayo de 2018.
- Manual de Políticas de Seguridad de Información del Senado de la Republica de Colombia código RT-MA02 Versión del 19 de septiembre de 2017.
- Norma Técnica Colombiana ISO 27001:2013 Sistemas de Gestión de la Seguridad de la Información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- 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, Por la cual se dictan disposiciones generales para la protección de datos personales.

	MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-M-02-02
		VERSIÓN: 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 17 DE 17
		FECHA: 21/10/2021

ANEXOS

AP-GI-PL-02 Plan de Gestión de Seguridad de la Información
 AP-GI-PL-03 Plan de tratamiento del riesgo de la información
 AP-GI-I-03 Instructivo generación copias de seguridad (backups)
 AP-GI-I-02 Instructivo administración de cuentas de usuario
 AP-GI-F-55 Control de acceso data center
 AP-GI-I-04 Instructivo uso recursos tecnológicos
 AP-AT-F-01 Traslado Devolutivos e inventarios

CONTROL DEL DOCUMENTO			
Versión	Fecha	Descripción de la modificación	Elaborado por:
1	07/02/2019	Creación	Nombre: Yolanda Ma. Cardozo H. Cargo: Profesional Universitario
2	21/10/2021	Se actualiza normatividad y se aplica nueva plantilla institucional, se modifica el contenido en general.	Nombre: Yolanda Bernal G. / Diego García - Diego García Cargo: Profesional Universitario / Apoyo Profesional Especializado

Revisado por:	Aval Oficina de Calidad:	Aval de Gestión Documental:	Aprobó:
Nombre: Álvaro Enrique Sossa Vivas	Nombre: Johana Patricia Sabogal Enríquez	Nombre: Martha Ligia Castillo Díaz	Nombre: Jaime Humberto García Hurtado
Cargo: Jefe Oficina Sistemas de Información - TIC	Cargo: Jefe Oficina de Calidad	Cargo: Líder Gestión Documental	Cargo: Gerente
ORIGINAL FIRMADO			