MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

CONTENIDO

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 para la gestión de la seguridad de la información, promoviendo el uso de mejores prácticas y mejorando la disponibilidad, integridad y confiabilidad de la información de la Subred Norte ESE, presentando en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred, bajo el liderazgo del Área de Sistemas de Información - TIC.

3. Alcance y Campo de Aplicación

El presente manual de políticas de seguridad de la información, se 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 Norte ESE.

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.

4. Marco Conceptual

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la entidad, y en consecuencia, debe ser protegido.
Acuerdo de Confidencialidad: documento en el que los funcionarios del Senado o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información del entidad, 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.
Amenaza: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.
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.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.
Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.
Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.
Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
Disponibilidad: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.
Gestión de claves: Controles referidos a la gestión de claves criptográficas.
Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
Impacto: Resultado de un incidente de seguridad de la información.
Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red1 o faciliten información con clasificación confidencial o superior. En el campo de la seguridad informática, es un método o forma de ataque con técnicas que buscan persuadir al atacado ganando su confianza, obteniendo información privilegiada de carácter personal (contraseñas de cuentas bancarias, datos personales), igualmente apropiarse de información vital para una organización. Existen en la actualidad diversidad de medios para llevar a cabo esta actividad, un uso común es a través de correos electrónicos o llamadas al lugar de trabajo o residencia, de ahí la importancia de tener una buena cultura digital respecto a que información suministramos.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No conformidad grave: Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/IEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.
Valoración de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.
Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.
Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4.1 Marco Legal

La Ley 599 de 2000 Capitulo VII	Por medio del cual se establecen las disposiciones relacionadas con la violación a la intimidad, reserva e interceptación de comunicaciones
La Directiva No. 005 de 2005 de la Alcaldía Mayor de Bogotá	Que establece la necesidad de aplicación por parte de las Entidades del Distrito Capital, de las políticas generales de tecnología de información y comunicaciones en su gestión informática
Acuerdo 279 de 2007	Establece lineamientos para la Política de Promoción y Uso del Software libre en el Sector Central, el Sector Descentralizado y el Sector de las Localidades del Distrito Capital
La Ley 1266 de 2008	Se dictan las disposiciones generales del habeas data y 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.
Resolución 305 de 2008	Resolución expedida por secretaria general del distrito en la cual se establece políticas públicas para las entidades del distrito capital, en materia de tecnologías de información y comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de datos espaciales y software libre.
La 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 los datos"** y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones
Del CONPES 3701 de 2011	Por el cual se establecen los lineamientos de políticas para la ciber-seguridad y ciber-defensa.
La Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales
Resolución no. 123 de 2012	Modifica el artículo 2° de la Resolución 1445 de 2006, sobre los Estándares de Acreditación para instituciones prestadoras de salud IPS. Con el fin de que los entes acreditadores certifiquen el nivel de calidad en la atención en las IPS, las Entidades Administradoras de Planes de Beneficios y las Direcciones Territoriales de Salud.
Del Decreto 2573 de 2014	mediante el cual se desarrollan los componentes y los tiempos de implementación de la estrategia GEL

La 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.
Del Decreto 1081 de 2015	Establece en su Capítulo 1 “Disposiciones generales" tiene por objeto reglamentar la Ley 1712 de 2014 en lo relativo a la gestión de la información pública.
La Ley 1753 de 2015 Artículo 45	por la cual se expide el Plan Nacional de Desarrollo 2014 - 2018 "Todos por un nuevo país" que señala que se deben establecer estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano
Del Decreto 1078 de 2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Del Conpes 3854 de 2016	se establecen los lineamientos y directrices de seguridad digital
Resolución 246 de 2016	Por la cual se dictan disposiciones en relación con el Sistema de Información para la Calidad y se establecen los indicadores para el monitoreo de la calidad en salud.
De la Circular 01 de 2017 de la Alta Consejería Distrital De TIC	Que enuncia los lineamientos de avance del modelo de seguridad y privacidad de la información
La norma BS 7799/ISO 17799	Para un mejor acercamiento a la seguridad de la información
Norma técnica colombiana NTC-ISO/IEC 17799	Código de buenas prácticas para la gestión de la seguridad de la información, 13 de diciembre de 2004
NTC-ISO/IEC: 27001, 27002, 27003, 27005	Norma técnica Colombiana Sobre Seguridad y Privacidad de la información.

5. Políticas

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

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para la **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE**, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad, el no repudio, la seguridad digital y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE**, para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad y privacidad información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- ✓ Minimizar el riesgo de los procesos misionales de la entidad.
- ✓ Cumplir con los principios de seguridad de la información.
- ✓ Cumplir con los principios de la función administrativa.
- ✓ Mantener la confianza de los funcionarios, contratistas y terceros.
- ✓ Apoyar la innovación tecnológica.
- ✓ Implementar el sistema de gestión de seguridad de la información.
- ✓ Proteger los activos de información.
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE**.
- ✓ Garantizar la continuidad del negocio frente a incidentes.

5.1.1 Alcance/Aplicabilidad

- ➢ Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** y la ciudadanía en general.

5.1.2 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política.

A continuación se establecen los 12 principios de seguridad que soportan el SGSI de la **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE**:

- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso

incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** protegerá su información de las amenazas originadas por parte del personal.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** implementará control de acceso a la información, sistemas y recursos de red.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- La **SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE ESE** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

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.

5.2 Política del tratamiento y trasferencia de datos

La Subred Integrada de Servicios de Salud Norte ESE asegura la confidencialidad y debido manejo de la información que obtenga, registre, use, transmita y actualice mediante autorización previa, expresa y voluntaria del titular de la información. Que lo anterior se desarrolla en estricto cumplimiento de la Ley Estatutaria 1581 de 2012 y su decreto reglamentario 1377 de 2013.

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.

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

5.2.1 Alcance

Esta Política aplica a la información personal que obtenga La Subred Integrada de Servicios de Salud Norte ESE en el desarrollo de actividades de prestación de servicios de salud, y en las actividades laborales, comerciales, académicas y de investigación relacionadas.

5.2.2 Definiciones en el ámbito de aplicación de la política de tratamiento de datos

Se entiende por:

a) **Autorización**: consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

b) **Base de datos**: conjunto organizado de datos personales que sea objeto de tratamiento.

c) **Dato personal**: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) **Aviso de privacidad**: Comunicación verbal o escrita generada por el Responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

e). **Dato público**: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

f) **Datos sensibles**: se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

g) **Encargado del tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

h) **Responsable del tratamiento**: persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos. h) Titular: persona natural cuyos datos personales sean objeto de tratamiento) Tratamiento: cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

i). **Transferencia:** La transferencia de datos tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

j). **Transmisión**: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del Responsable.

5.2.3 Del Titular

Para efectos de esta Política se entenderán como titulares de datos personales, personas naturales o jurídicas entre ellas los pacientes y usuarios del servicio de salud, los proveedores, clientes, benefactores, estudiantes, profesionales de la salud y empleados en general.

5.2.4 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 al Titular se debe informar de manera clara la finalidad para la cual se recaudan los datos personales, el tratamiento al cual pueden ser sometidos los datos personales, 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

La autorización para el tratamiento de los datos personales de menores de edad debe realizarse bajo la facultad de los padres de familia o representantes legales del menor.

5.2.5 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 le 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.

5.2.5.1 Derechos de los niños y Adolescentes

En el tratamiento de datos personales se asegurará el respeto a los derechos prevalentes de los menores. Queda proscrito el tratamiento de datos personales de menores, salvo aquellos datos que sean de naturaleza pública, y en este caso el tratamiento deberá cumplir con los siguientes parámetros:

a. Responder y respetar el interés superior de los menores
b. Asegurar el respeto de los derechos fundamentales de los menores.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del Tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

5.2.6 Deberes del titular

El Titular debe garantizar la veracidad de la información que proporciona a la Subred Integrada de Servicios de Salud Norte ESE y actualizar su información de manera oportuna. En caso de falsedad en la información suministrada la Subred Integrada de Servicios de Salud Norte ESE se exime de cualquier responsabilidad.

5.2.7 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 (571) 3499080
www.subrednorte.gov.co

5.2.8 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.

5.2.9 Tipo de información registrada

Para facilitar el contacto con los Titulares, registramos y conservamos 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
- En los procesos de atención asistencial
- En los procesos de facturación de servicios
- Otras fuentes, que brindan información relacionada con el servicio que el usuario requiere.
- En los procesos de actividades financieros
- En desarrollo de actividades educativas
- En el ejercicio de procesos laborales

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 nuestra institución prestadora de servicios de salud, también registramos 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; 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 auditorias, relacionamiento comercial, procesamiento y verificación de medios de pago, correspondencia de nuestra 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 nuestro 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.

5.2.10 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 bancarias o bursátiles, conforme a la legislación que les resulte aplicable;

d) Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad;

e) 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.

5.2.11 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

5.2.12 Procedimientos para consultas y reclamos

Consultas: Las consultas realizadas por el Titular o sus causahabientes serán atendidas por la Subred Integrada de Servicios de Salud Norte ESE en un término de (10) días hábiles a partir del recibo de la solicitud prorrogable por un término máximo de (5) días hábiles

Reclamos: El Titular o sus causahabientes que consideren que la información contenida en la base de datos de la Subred Integrada de Servicios de Salud Norte ESE debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley o en esta política, podrán presentar un reclamo ante el área de Atención al Usuario, el cual será tramitado bajo las siguientes reglas:

El reclamo se formulará mediante solicitud dirigida a la Oficina de Participación Comunitaria y Servicio al Ciudadano de la Subred Integrada de Servicios de Salud Norte ESE, por correo convencional, a la Calle 66 No. 15-41 Bogotá D.C. Colombia, con la identificación del Titular, la descripción de los hechos que dan lugar al reclamo, la dirección, y acompañando los documentos que se quieran hacer valer.

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo, el cual se podrá prorrogar por un término máximo de ocho (8) días hábiles

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días hábiles siguientes a la recepción del reclamo para que subsane las fallas. Si transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Antes de acudir a la entidad encargada de vigilar el cumplimiento de las normas sobre protección de datos personales, el Titular debe tramitar inicialmente su reclamo con la Subred Integrada de Servicios de Salud Norte ESE a través de los medios y canales dispuestos para tal fin.

5.2.13 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.

5.2.14 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.

5.3 Política de uso de Activos de Información

5.3.1 Objetivo

Lograr y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

5.3.2 Alcance

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.

5.3.3 Normas del uso de los Activos de Información

- Los activos de información pertenecen a la Subred Integrada de Servicios de Salud Norte ESE y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Toda la información sensible de la Subred Norte ESE, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte el área de Recursos Físicos e Inventarios. Los propietarios de los activos de información

deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área de sistemas de información- TIC.
- La Servicios de Salud Norte ESE proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Subred Norte ESE, los funcionarios solo podrán realizar copias de seguridad (backup) de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por la subred; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.
- Periódicamente, el Área de Sistemas de la Información- TIC efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considera como una violación a las Políticas de Seguridad de la Información de la Subred Norte ESE.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Jefe inmediato de cada proceso o el director a través de la mesa de servicio o ayuda del Área Sistemas de Información- TIC.
- Estarán bajo custodia del Área de Sistemas de la Información- TIC los medios magnéticos/electrónicos (CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los *passwords o contraseñas* de administración de los equipos, sistemas de información o aplicativos.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de ***redes sociales personales***, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Tecnología y Sistemas de la Información:
    - Instalar software en cualquier equipo de la Subred Norte ESE.
    - Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la Subred Norte ESE.
    - Modificar, revisar, transformar o adaptar cualquier software propiedad de la Subred Norte ESE.
    - Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Subred Norte ESE.
    - Copiar o distribuir cualquier software de propiedad de la Subred Norte ESE.
    - Cambiar la configuración de hardware de propiedad de la Subred Norte ESE.
- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de la Subred.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
    - Ningún usuario deberá acceder a la red o a los servicios TIC de la Subred, utilizando una cuenta de usuario o clave de otro usuario.

- Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem, USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos de la Subred Norte ESE.

5.4 Política para uso de dispositivos móviles institucionales (celulares – tables-USB)

5.4.1 Objetivo

Proveer las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, USB, entre otros) institucionales y personales que hagan uso de servicios de la institución. Así mismo, velará porque los funcionarios hagan un uso responsable de los servicios y equipos proporcionados por la entidad.

5.4.2 Alcance

Estas son políticas que aplican a la todos los funcionarios y en general se aplicara a todos los directivos, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred Norte ESE, que tengan asignado un dispositivo.

5.4.3 Normas para el uso de dispositivos móviles

- Los usuarios deben evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.
- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales bajo su responsabilidad, ni desinstalar el software provisto con ellos al momento de su entrega.
- Los usuarios deben evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.
- Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Área de Sistema de Información-TIC, realizar el debido denuncio ante las autoridades competentes, y continuar con el procedimiento administrativo por perdida de elementos establecido por la entidad.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Subred Norte ESE con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.
- Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.

5.5 Política de uso adecuado del Internet

5.5.1 Objetivo

Establecer directrices que permitan a los usuarios de la Subred Norte ESE la navegación segura y su uso adecuado, evitando errores, pérdidas, modificaciones no autorizadas de la información en las aplicaciones WEB.

5.5.2 Alcance

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.

5.5.3 Normas de uso adecuado de internet

- 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.
- El área de sistemas de información-TIC debe monitorear continuamente el canal o canales del servicio de Internet.
- El área de sistemas de información-TIC debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El área 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 expresa del comité de seguridad y privacidad de la Información de la Subred Norte ESE.
- El Área de Tecnología Sistemas de Información - TIC administrará autorización de navegación a los usuarios de la Subred Norte ESE, previa solicitud del Jefe inmediato.
- El área 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.
- El uso de internet no está para escuchar emisoras en línea, ver videos no institucionales en youtube, acceder a transmisiones de eventos deportivos, políticos, películas, juegos, etc, solo está para fines institucionales y misionales.

5.6 Política de escritorio y pantalla limpia

5.6.1 Objetivo

Definir los lineamientos básicos para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios de sus escritorios y evitar ralentizar el rendimiento del navegador en los equipos de cómputo de la Subred Norte ESE.

5.6.2 Alcance

Motivar una mejor organización y productividad que brinde seguridad y disponibilidad, cuando el escritorio de todos los equipos o estaciones de trabajo están limpios y todas las áreas de la Subred Norte ESE están libres de papeles atendiendo a las disposiciones del área de Gestión Documental de la Subred y la eficiencia administrativa. Por lo anterior aplica a todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred.

5.6.3 Normas de escritorio limpio

- Ubicar los escritorios de manera que impida que impida que terceras personas puedan ver la información de la pantalla.
- La información en la que se está trabajando tanto en medio magnético como físico en los puestos de trabajo es de propiedad de la Subred Integrada de Servicios de Salud Norte ESE
- Cada vez que se generen ausencias del puesto de trabajo, por tiempo prolongado, se debe asegurar que la información usada quede fuera del alcance de terceras personas bloqueando el escritorio y el uso de usuario / contraseñas las cuales no deben ser compartidas entre los usuarios, en caso de requerirse el ingreso al equipo de cómputo el usuario/ contraseña lo debe conocer el jefe inmediato.
- Los usuarios a los que la subred Norte ESE les asigne equipos móviles como computadores, teléfonos inteligentes, tablets, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.
- Al imprimir documentos con información pública reservada y/o pública clasificada (semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
- No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos, cada uno de estos equipos cuenta con un responsable y es quien debe asegurar que no se pierda o extraiga de manera ilegal la información que es de propiedad de la Subred Norte ESE.
- La información pública reservada o información pública clasificada (privada o semiprivada) que se encuentre en medio físico, debe permanecer almacenada en una caja fuerte o gabinete de seguridad.
- Está prohibido tener sustancias o líquidos en su escritorio, los que pueden dañar los equipos, así como la documentación
- Todos los equipos deberán tener una protección contra accesos no autorizados.
- No dejar dispositivos de respaldo de información, como USB, Pendrive, CD, DVD, etc, a la mano de cualquier persona.
- No escribir contraseñas ni otros datos sensibles en papeles o documentos que queden a la vista.

- El usuario es responsable de cerrar su sesión de trabajo y dejar el equipo en suspensión, cuando deje de usarlo por tiempo prolongado.
- Desde el momento en que firma el acta de asignación de un equipo, la responsabilidad sobre el estado del equipo, es totalmente del usuario.

5.7 Política de uso de correo electrónico

5.7.1 Objetivo

La Subred Integrada de Servicios de Salud Norte ESE busca proporcionar un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

5.7.2 Alcance

El servicio de correo electrónico permite a los usuarios de la Subred Norte ESE, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones, por tal razón estas políticas se aplicaran a todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Subred.

5.7.3 Normas de uso del correo electrónico

- Los usuarios del correo electrónico institucional son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los servicios de correo electrónico institucional se emplean para servir a una finalidad operativa y administrativa en relación con la entidad.
- Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la Subred Norte ESE se consideran bajo el control de la entidad.
- El área de Sistemas de información - TIC debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes, así mismo garantizar el respaldo de la información sea a través de un proveedor o si es local garantizando la infraestructura adecuada para tal fin.
- La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario de la Subred, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
- Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional de la Subred.
- El correo institucional no debe ser utilizado para actividades personales.
- Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios de la Subred Norte ESE. No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

- Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Subred Norte ESE y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad y de medio ambiente.

5.8 Política de seguridad para los equipos institucionales

5.8.1 Objetivo

Asegurar la protección de la información en los equipos de cómputo y establecer las reglas para proteger las operaciones correctas y de procesamiento de la Subred Integrada de Servicios de Salud Norte ESE, con el fin de garantizar la continuidad de los sistemas de Información con el apoyo de las TIC.

5.8.2 Alcance

Estos lineamientos deben ser aplicados por todos los funcionarios, contratistas y demás personal de la Subred Integrada de Servicios de Salud Norte ESE.

5.8.3 Normas de uso de seguridad para equipos institucionales

Con relación a la instalación de equipos de cómputo y almacenamiento, los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Área de Sistemas de Información - TIC.

Para las protecciones en el suministro de energía a la red regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, monitores; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el Área de Recursos Físicos. El Área de Recursos Físicos de la Subred Integrada de Servicios de Salud Norte ESE debe implementar sistemas redundantes de alimentación eléctrica, como por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de energía.

Con respecto a la Seguridad del cableado, los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas. Deben existir planos que describan las conexiones del cableado. El acceso a los centros de cableado (Racks), debe estar protegido. El Área de Sistemas de Información - TIC establece un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

Mantenimiento de los Equipos: La Subred Integrada de Servicios de Salud Norte ESE, debe mantener contratos de soporte y mantenimiento de los equipos críticos. Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento, en el caso de las cámaras de seguridad, aires acondicionados y de precisión, sistema de detección y extinción de incendios, UPS, Plantas Generadoras de Energía, mantenimiento de cableados de datos y redes eléctricas, deberá ser asumido por el Área de Recursos Físicos.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas y realizadas por personal autorizadas por el Área de Sistemas de Información - TIC.

Los equipos que requieran salir de las instalaciones de la Subred Norte ESE para reparación o mantenimiento, deben estar debidamente autorizados por el Área de Activos Fijos y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada). Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos de la entidad, teniendo en cuenta los diferentes riesgos que se pueden presentar al trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de la Subred Norte ESE. Los equipos retirados de la entidad deben ser protegidos**, no se deben dejar sin vigilancia en lugares públicos**, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del área de Activos fijos y de Sistemas de Información- TIC, así mismo debe garantizarse la copia y eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando las herramientas adecuadas para estos procesos.
A los equipos de cómputo se les deben realizar mantenimientos preventivos según el plan de mantenimiento se realizaran dos al año uno en cada semestre.

Equipo Informático de Usuario Final desatendido el área de Sistemas de Información – TIC debe asegurar que todos los equipos de cómputo de la Subred Integrada de Servicios de Salud Norte ESE se encuentren en un único dominio de red, en caso contrario se deberá prestar la protección adecuada.

Con relación a los puestos de Trabajo y con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios, contratistas y terceros de la Subred Integrada de Servicios de Salud Norte ESE, deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye documentos impresos, CD, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todos los equipos de cómputo deberán usar el papel tapiz y el protector de pantalla que establezca la entidad. No se debe utilizar fotocopiadoras, escáneres, cámaras digitales, y en general equipos tecnológicos que se encuentren desatendidos.

6. BIBLIOGRAFÍA

El presente Manual de Políticas de Seguridad y Privacidad de la Información se realizó en 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 27000:2013 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.

ANEXOS

AP-GI-PL-03-01-PLAN DE TRATAMIENTO DEL RIESGO DE LA INFORMACIÓN
AP-GI-PL-02-01-PLAN DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CONTROL DEL DOCUMENTO			
Versión	**Fecha**	**Descripción de la modificación**	**Realizada por**
1	07/02/2019	Creación	Nombre: Yolanda Ma. Cardozo H. Cargo: Profesional Universitario

Elaboró:	**Revisó:**	**Aval técnico de normalización:**	**Aprobó:**
Nombre: Víctor Julio Gómez Carvajal	Nombre: María Eugenia Rodríguez	Nombre: Martha Ligia Castillo Díaz	Nombre: Yidney Isabel García Rodríguez
Cargo: Jefe Oficina Sistemas de Información - TIC	Cargo: Jefe Oficina de Calidad	Cargo: Líder Gestión Documental	Cargo: Gerente Subred Integrada de Servicios de Salud Norte ESE
ORIGINAL FIRMADO			