

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 1 DE 19
		FECHA: 07/02/2019

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

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

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 2 DE 19
		FECHA: 07/02/2019

CONTENIDO

1. INTRODUCCIÓN	3
2. JUSTIFICACIÓN	3
3. ALCANCE	4
4. OBJETIVOS	4
4.1 Objetivo General	4
4.2 Objetivos Específicos	4
5. MARCO NORMATIVO	5
5.1 Normatividad Nacional	5
5.2 Normatividad Internacional	10
5.3 Buenas Prácticas	12
6. VOCABULARIO	14
7. DESARROLLO	16
7.1 Planeación	16
7.2 Hacer	17
7.3 Verificar	17
7.4 Actuar	17
8. SEGUIMIENTO Y MEDICIÓN	18
9. BIBLIOGRAFÍA	18
ANEXOS	19

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 3 DE 19
		FECHA: 07/02/2019

1. INTRODUCCIÓN

La nueva Política de Gobierno Digital tiene el objetivo de desarrollar un enfoque integral que permita obtener, por medio del uso y aprovechamiento de las tecnologías de la información, un valor público mediante la articulación entre el Estado y la Sociedad generando mayor competitividad, innovación y proactividad.

La Política de gobierno digital está conformada por dos (2) componentes denominados, **TIC para el Estado y TIC para la Sociedad**, ambos encargados de orientar la implementación de esta política, además de tres (3) habilitadores transversales que facilitan su desarrollo, llamados:

- Seguridad y Privacidad
- Arquitectura de Tecnologías de la Información-TI
- Servicios Ciudadanos Digitales

Estos habilitadores se desarrollaran en los cinco (5) propósitos definidos en la política, como son:

- Servicios Digitales,
- Procesos Internos Seguros y Eficientes
- Decisiones Basadas en Datos
- Empoderamiento Ciudadano
- Desarrollo de territorios y Ciudades Inteligentes

En este plan se hace referencia al habilitador de Seguridad y Privacidad, por lo cual es necesario hablar del Modelo de Seguridad y Privacidad de la Información que hace parte de la antigua estrategia Gobierno en Línea – GEL. En este modelo se propone un conjunto de guías prácticas que contribuyen a mitigar los riesgos asociados a la seguridad y privacidad de la información, así como velar por la preservación de la confidencialidad, integridad y disponibilidad de los activos de información con los que cuenta la Entidad.

En tal sentido, la seguridad y privacidad de la información actúa como eje transversal e integral para el desarrollo de objetivos así mismo se alinea con las dos políticas del **Modelo Integrado de Planeación y Gestión – MIPG**, Gobierno Digital y Seguridad Digital.

2. JUSTIFICACIÓN

Con la transformación de la Estrategia de Gobierno en Línea a política de Gobierno Digital, obliga a la entidad a resolver nuevos retos encaminados hacia la implementación de cada uno de los componentes, habilitadores y el logro de los propósitos que hacen parte de la nueva política “Gobierno Digital”. Como respuesta a los requerimientos de la política digital y a lo establecido el Decreto 1008 del 14 de junio de 2018 de MinTIC : “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones” la Subred Integrada de Servicios de Salud Norte ESE, va a desarrollar el habilitador seguridad y privacidad de la información utilizando la metodología definida por el MinTIC.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 4 DE 19
		FECHA: 07/02/2019

De igual forma y en cumplimiento de las dos políticas establecidas en el Modelo Integrado de Planeación y Gestión - MIPG, las cuales son Gobierno Digital y Seguridad Digital la Subred Integrada de Servicios de Salud Norte ESE alineara este plan para su respectiva adopción.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información inicia con la definición y adopción del Manual de políticas de seguridad de la información, la clasificación y definición de los responsables de los activos de información que hacen parte de los procesos, la identificación y tratamiento de los riesgos de seguridad de la información y finaliza con la definición de procedimientos, controles y buenas prácticas de seguridad de la información que permitan proteger los activos de información de la Subred Integrada de Servicios de Salud Norte ESE

4. OBJETIVOS

4.1 Objetivo General

Incorporar la seguridad de la información en todos los procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de Subred Integrada de Servicios de Salud Norte ESE, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este Objetivo se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.

4.2 Objetivos Específicos

- Establecer los procedimientos, controles y buenas prácticas para la gestión de eventos e incidentes que afecten la integridad, confidencialidad e integridad de los activos de información de la entidad.
- Definir políticas y controles que contribuyan con la seguridad y privacidad de la información de la entidad.
- Identificar acciones de mejora que faciliten el intercambio de información pública de forma segura.
- Sensibilizar el talento humano para la gestión eficiente y eficaz en seguridad y privacidad de la información.
- Establecer medidas de implementación y de verificación de los controles previstos en el Modelo de Seguridad y Privacidad de la Información con base en el Plan de riesgos de seguridad y privacidad de la información identificada en la entidad.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 5 DE 19
		FECHA: 07/02/2019

5. MARCO NORMATIVO

5.1 Normatividad Nacional

Normatividad Nacional sobre Seguridad y Privacidad de la Información	
Constitución Política de Colombia, en sus Artículos 11, 12, 13, 14, 17, 21, 22, 24, 29, 44, entre otros.	Por ejemplo, Art. 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.
Ley 527 de 1999 (Comercio Electrónico)	Por medio de la cual se define y se reglamenta el acceso y uso de los mensajes de datos, el comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Se tratan conceptos como: mensaje de datos (artículos 2º y 5º), el principio de equivalencia funcional (artículos 6º, 8º, 7º, 28º, 12º y 13º), la autenticación electrónica (artículo 17º), la firma electrónica simple (artículo 7º), la firma digital (artículo 28º), y la firma electrónica certificada (artículo 30º, modificado por el artículo 161 del Decreto Ley 019 de 2012).
Ley 594 de 2000 (Ley General de Archivos)	Habilita el uso de nuevas tecnologías de manera general, es posible establecer que para satisfacer los requerimientos establecidos en esta norma sea viable usar firmas electrónicas simples, certificadas y firmas digitales.
Ley 599 de 2000 (Código Penal)	Por la cual se expide el código penal colombiano.
Ley 600 de 2000 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal.
Ley 679 de 2001 (Pornografía y explotación sexual con menores)	Esta Ley contempla en el artículo 4, un sistema de autorregulación, en virtud del cual el Gobierno nacional, por intermedio del Ministerio de Comunicaciones hoy Ministerio de Tecnologías de la Información y las Comunicaciones, promoverá e incentivará la adopción de sistemas de autorregulación y códigos de conducta eficaces en el manejo y el aprovechamiento de redes globales de información, estos códigos se elaboraran con la participación de organismos representativos de los proveedores y usuarios de servicios de redes globales de información.
Ley 906 de 2004 (Código de Procedimiento Penal)	Por la cual se expide el código de procedimiento penal (corregida de conformidad con el Decreto 2770 de 2004

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 6 DE 19
		FECHA: 07/02/2019

Normatividad Nacional sobre Seguridad y Privacidad de la Información	
Ley 962 de 2005 (racionalización de trámites y procedimientos)	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1032 de 2006 (derechos de autor y conexos)	Por la cual se modifican los artículos 257, 271, 272 y 306 del código penal (artículo 271. violación a los derechos patrimoniales de autor y derechos conexos).
Ley 1150 de 2007 (medidas para la eficiencia y la transparencia)	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública (SECOP).
Circular Externa SFC 052 de 2007	Por la cual la Superintendencia Financiera de Colombia incrementa los estándares de seguridad y calidad para el manejo de la información a través de medios y canales de distribución de productos y servicios que ofrecen a sus clientes y usuarios las entidades vigiladas por esta Entidad
Ley 1266 de 2008 (Habeas Data)	Contempla las disposiciones generales en relación al derecho de habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
Ley 1273 de 2009 (Delitos Cibernéticos)	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 TIC"
Ley 1341 de 2009 (Sector TIC)	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones
Decreto 1727 de 2009 (Habeas Data)	Se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 7 DE 19
		FECHA: 07/02/2019

Normatividad Nacional sobre Seguridad y Privacidad de la Información	
Decreto 2952 de 2010 (Habeas Data)	Este Decreto reglamenta los artículos 12 y 13 de la Ley 1266 de 2008, en este sentido establece que con fundamento en el principio constitucional de solidaridad surgen obligaciones a cargo del Estado y de los ciudadanos, en virtud de las cuales cuando se presenten situaciones de fuerza mayor, es posible otorgar a las víctimas de secuestro, desaparición forzada y personas secuestradas, debido a su estado de debilidad manifiesta, un tratamiento diferenciado en la administración de su información financiera, crediticia y comercial.
Ley 1437 de 2011 (Uso de medios electrónicos Procedimiento Administrativo Electrónico)	Consagra la utilización de medios electrónicos en el procedimiento administrativo permitiendo adelantar los trámites y procedimientos administrativos por medios electrónicos, el uso de registros electrónicos, de documentos públicos en medios electrónicos, notificaciones electrónicas, archivos electrónicos de documentos, expedientes electrónicos y sedes electrónicas. Lo anterior, con el fin de que los ciudadanos interactúen por medios electrónicos con validez jurídica y probatoria.
Ley 1453 de 2011 (Estatuto de seguridad ciudadana)	Por medio de la cual se reforma el código penal, el código de procedimiento penal, el código de infancia y adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad.
Ley 1474 de 2011 (Uso de medios tecnológicos)	Esta norma permite la utilización de medios tecnológicos en los trámites y procedimientos judiciales, en las diligencias, práctica de pruebas y notificaciones de las decisiones.
Ley 1564 de 2011 (Uso de las TIC)	Permite el uso de las TIC en todas las actuaciones de la gestión y trámites de los procesos judiciales con el fin de facilitar el acceso a la justicia.
Ley 1581 de 2012 (Habeas Data)	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley 1712 de 2012 (Uso de las TIC y Transparencia)	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 8 DE 19
		FECHA: 07/02/2019

Normatividad Nacional sobre Seguridad y Privacidad de la Información	
Decreto Ley 019 de 2012 (Entidades de Certificación Digital)	Establece las siguientes actividades que las entidades de certificación acreditadas podrán realizar en el país, tales como emitir certificados en relación con las firmas electrónicas o digitales de personas naturales o jurídicas, emitir certificados sobre la verificación respecto de la alteración entre el envío y recepción del mensaje de datos y de documentos electrónicos transferibles, y emitir certificados en relación con la persona que posea un derecho u obligación con respecto a los documentos enunciados en los literales f) y g) del artículo 26 de la Ley 527 de 1999, entre otras.
Resolución SIC No. 76434 de 2012 (Habeas Data)	Resolución expedida por la SIC, por medio de la cual se imparten instrucciones relativas a la protección de datos personales, en particular acerca del cumplimiento de la Ley 1266 de 2008, sobre reportes de información financiera, crediticia, comercial de servicios y la proveniente de terceros países.
Decreto 2364 de 2012 (Firma electrónica)	Establece la reglamentación del artículo 7º de la Ley 527 de 1999, complementando el marco jurídico de los mecanismos de autenticación previstos en Colombia. Se definen algunas características que benefician el uso de los medios electrónicos, tales como la definición de los criterios de confiabilidad y apropiabilidad en el uso de los mecanismos de autenticación, la fijación de la relación de género y especie entre firmas electrónicas y firmas digitales, señalando las diferencias en su tratamiento probatorio, pues en el último mecanismo existe una inversión probatoria, y el uso de la firma electrónica mediante acuerdo de las múltiples partes de una relación jurídica, entre otras.
Decreto 1377 de 2013 (Habeas Data)	Se reglamenta parcialmente la Ley 1581 de 2012, facilitando la implementación y el cumplimiento de la Ley 1581 de 2012, reglamentando aspectos particulares relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, además consagra políticas de tratamiento de los responsables y encargados.
Decreto 333 de 2014 (Habeas Data)	Se reglamenta el artículo 160 del Decreto 019 de 2012), definiendo el régimen de acreditación de las entidades de certificación abierta, en desarrollo de lo que define el artículo 160 del Decreto 019 de 2012 y se deroga el Decreto 1747 de 2000, que reglamenta de manera parcial la Ley 527 de 1999, referente a las entidades de certificación digital, certificados y firmas digitales, de manera que las entidades que deseen seguir prestando los servicios de certificación digital, deberán iniciar la correspondiente acreditación, ya no ante la Superintendencia de Industria y Comercio, sino ante el Organismo de Acreditación en Colombia (ONAC).

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 9 DE 19
		FECHA: 07/02/2019

Normatividad Nacional sobre Seguridad y Privacidad de la Información	
Decreto 886 de 2014 (Registro Nacional de Base de Datos)	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al registro nacional de bases de datos. Se reglamenta la información mínima que debe contener dicho registro, creado por la Ley 1581 de 2012, así como los términos y condiciones bajo las cuales se deben inscribir en este los responsables del tratamiento.
Decreto 2573 de 2014 (Gobierno en Línea)	Por el cual se establecen los lineamientos generales de la estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector TIC)	Por medio del cual se expide el Decreto único reglamentario del sector TIC, el cual tiene por objeto compilar las normas reglamentarias preexistentes que rigen el sector.
Circular Externa SIC 02 del 3 de noviembre de 2015	Por la cual la Superintendencia de Industria y Comercio impartió instrucciones a los responsables del tratamiento de datos personales, personas jurídicas de naturaleza privada inscritas en las cámaras de comercio y sociedades de economía mixta, para efectos de realizar la inscripción de sus bases de datos en el registro nacional de bases de datos a partir del 9 de noviembre de 2015.
CONPES 3701 de 2011	Dicta lineamientos de políticas para ciberseguridad y ciberdefensa
CONPES 3854 de 2016	Incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 10 DE 19
		FECHA: 07/02/2019

5.2 Normatividad Internacional

Normatividad Internacional sobre Seguridad y Privacidad de la Información	
Convenio sobre Ciberdelincuencia del Consejo de Europa CCC (conocido como el convenio sobre Cibercriminalidad de Budapest) Adoptado en noviembre de 2001 y entrada en vigor desde el 1° de julio de 2004	El objetivo principal del convenio es la adopción de una legislación que facilite la prevención de las conductas delictivas y contribuya con herramientas eficientes en materia penal que permitan detectar, investigar y sancionar las conductas antijurídicas.
Resolución AG /RES 2004 (XXXIV-O/04) de la Asamblea General de la Organización de los Estados Americano	Se establece una estrategia Integral para combatir las amenazas a la seguridad cibernética con un enfoque multidimensional y multidisciplinario para la creación de una cultura de la seguridad cibernética. Se estipulan tres vías de acción: i) Creación de una Red Hemisférica de CSIRT, cometido asignado al CICTE de la OEA; ii) Identificación y adopción de normas técnicas para una arquitectura segura de Internet, labor desarrollada por la Comisión Interamericana de Telecomunicaciones; y iii) Adopción o adecuación de los instrumentos jurídicos necesarios para proteger a los usuarios de Internet y las redes de información de los delincuentes y los grupos delictivos organizados que utilizan estos medios, a cargo de las Reuniones de Ministros de Justicia o de Ministros o Procuradores Generales de las Américas - REMJA.
Decisión 587 de la Comunidad Andina, adoptada el 10 de julio de 200	Por la cual se establecen los lineamientos de la Política de Seguridad Externa Común Andina. Dentro de los objetivos de dicha política se encuentra el prevenir, combatir y erradicar las nuevas amenazas a la seguridad y cuando corresponda sus interrelaciones, a través de la cooperación y coordinación de acciones orientadas a enfrentar los desafíos que representan dichas amenazas para la Comunidad Andina.
Consenso en materia de ciberseguridad de la Unión Internacional de Telecomunicaciones - UIT, en el seno de Naciones Unidas, en desarrollo del programa de acciones de Túnez para la sociedad de la información de 2005	Busca la promoción del examen de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Las Resoluciones que emita la UIT son vinculantes para Colombia, puesto que a través de las Leyes 252 de 1995 y 873 de 2004, se aprobó la constitución de la UIT y el Convenio de la UIT, así como las enmiendas posteriores que se han realizado.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 11 DE 19
		FECHA: 07/02/2019

Normatividad Internacional sobre Seguridad y Privacidad de la Información	
Resolución 64/25 "Los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional." Asamblea General de las Naciones Unidas (UNGA). (2009)	La Asamblea General exhorta a los Estados miembros a seguir promoviendo el examen multilateral de las amenazas reales y potenciales en el ámbito de la seguridad de la información y de posibles medidas para limitar las amenazas que surjan en ese ámbito, de manera compatible con la necesidad de preservar la libre circulación de información.
Directiva 2006/24 de la Unión Europea	Se establece la conservación de datos en la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, y fue el referente aplicado por los países miembros hasta el año 2014.
Pronunciamientos de Principios	Resoluciones UNGA: 55/63 y 56/121 sobre la lucha contra el uso delictivo de tecnologías de información; 57/239, 58/199 y 64/211 sobre la creación de una cultura mundial de seguridad cibernética y la protección de infraestructuras críticas de información; Cumbre Mundial sobre la Sociedad de la Información (CMSI), Declaración de Principios y Orden del Día de la Fase de Túnez (en particular la línea de acción C5). Estas son normas o principios generales, que no constituyen reglas y no son vinculantes, sin embargo estos actos o instrumentos jurídicos sin carácter obligatorio, son incardinados de una forma u otra, en el sistema de fuentes del Derecho Internacional (Soft Law).
Marco de trabajo de estrategias nacionales de ciberseguridad. Manual de la OTA	LA OTAN publica en el año 2012 en colaboración con la NATO Cooperative Cyber Defence Centre of Excellence el manual para la formulación de estrategias nacional de ciberseguridad para sus países miembros.
Declaración de la Cumbre de Gales de la OTAN en 201	Documento oficial de los resultados de la Cumbre de la OTAN celebrada en Cardiff (Gales) los días 4 y 5 de septiembre de 2014, en donde se resaltan acuerdos para abordar la ciberseguridad en los países de dicha alianza.
Declaración sobre la protección de infraestructura crítica ante las amenazas emergentes (Aprobado durante la quinta sesión plenaria, celebrada el 20 de marzo de 2015)	Declaración en donde, entre otros, la Secretaría Ejecutiva del CICTE de la OEA desarrolla un proyecto de asistencia técnica que, permita a estos la elaboración de un listado de su infraestructura crítica y su clasificación, basados en sus respectivos activos, sistemas, redes y funciones esenciales, para hacer posible la mejor evaluación de vulnerabilidades, brechas, amenazas, riesgos e interdependencia.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 12 DE 19
		FECHA: 07/02/2019

Normatividad Internacional sobre Seguridad y Privacidad de la Información	
Declaración sobre Seguridad en las Américas de la OEA (México, 2003)	Identifica como relevantes, entre otras nuevas amenazas, el terrorismo y los ataques a la seguridad cibernética, y comprometió a los Estados miembros a desarrollar una cultura de seguridad cibernética en las Américas con la adopción de medidas de prevención eficaces para prever, enfrentar y responder a los ataques cibernéticos, cualquiera fuera su origen, luchando contra las amenazas y la delincuencia cibernética, tipificando los ataques contra el espacio cibernético, protegiendo la infraestructura crítica y asegurando las redes de los sistemas

5.3 Buenas Prácticas

Estándares	Descripción
BICSI 002 (BICSI, 2014)	Mejores prácticas de diseño e implementación de Centros de Cómputo. Considerada la norma base para el diseño de centros de datos alrededor del mundo. ANSI/BICSI 002-2014 continúa su misión de proporcionar requisitos, directrices y mejores prácticas aplicables a cualquier centro de datos.
COBIT (ISACA, 2018)	Objetivos de control para tecnologías de la información y relacionadas. Denominado COBIT por sus siglas en inglés: Control Objectives for Information and related Technology.
ISO 21827 (ISO, 2008)	Modelo de Capacidad de Madurez en la seguridad de la información.
ISO/IEC 24764 (2010)	Especifica el cableado genérico que admite una amplia gama de servicios de comunicaciones para su uso dentro de un centro de datos. Cubre el cableado balanceado y el cableado de fibra óptica. Se basa en los requisitos de referencia de ISO / IEC 11801 y contiene requisitos adicionales que son apropiados para los centros de datos en los que la distancia máxima a la que deben distribuirse los servicios de comunicaciones es de 2.000 m.
ISO/IEC 27001:2013 (Icontec, 2013)	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 13 DE 19
		FECHA: 07/02/2019

ISO-IEC 27002:2013 (Icontec, 2015)	Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información
ISO/IEC 27000:2018 (ISO/IEC, 2018b)	Proporciona una visión general de los sistemas de gestión de seguridad de la información (SGSI). También proporciona términos y definiciones.
ISO/IEC 27005:2018 (ISO/IEC, 2018a)	Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información. Proporciona pautas para la gestión de riesgos de seguridad de la información.
ISO 31000:2018 (Icontec, 2018)	Gestión del riesgo. Directrices. Proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto.
ITIL (AXELOS, 2011)	Biblioteca de infraestructura de tecnología de la información, ITIL por sus siglas en inglés: Information Technology Infrastructure Library. Es el enfoque más ampliamente aceptado para la gestión de servicios de TI en el mundo.
Magerit versión 3 (Ministerio de Hacienda y Administraciones Públicas de España, 2012)	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.
Marco de trabajo de ciberseguridad de la NIST (National Institute of Standards and Technology, 2014)	Marco voluntario consta de estándares, directrices y mejores prácticas para gestionar el riesgo relacionado con la seguridad cibernética del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio del Gobierno Estadounidense -NIST, por sus siglas en inglés National Institute of Standards and Technology-.
Modelo Abierto de Madurez de la Gestión de la Seguridad de la Información (The open group, 2018a)	Modelo Abierto de Madurez de la Gestión de la Seguridad de la Información del “The Open Group”, una comunidad ampliamente reconocida por las buenas prácticas y estándares que han aportado a la industria de las TIC.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 14 DE 19
		FECHA: 07/02/2019

PTES Standard (PTES, 2012)	Estándar de ejecución de pruebas de penetración consta de siete (7) secciones principales. Estos cubren todo lo relacionado con una prueba de penetración, desde la comunicación inicial y el razonamiento detrás de un pentest, a través de la recopilación de inteligencia y las fases de modelado de amenazas en las que los evaluadores trabajan entre bambalinas para comprender mejor a la organización probada, a través de la investigación de vulnerabilidad.
NIST-800-30 (Stoneburner, Goguen, & Feringa, 2002)	Guía de gestión de riesgos para los sistemas de tecnología de la información. Publicación especial del Instituto Nacional de Estándares y Tecnología del Departamento de Comercio del Gobierno Estadounidense -NIST, por sus siglas en inglés National Institute of Standards and Technology-.
NIST-800-39 (Locke & Gallagher, 2011)	Publicación especial del NIST: Gestión de riesgos de seguridad de la información. Organización, misión y sistema de información.
NIST-800-53r5 (Ross & Rochford, 2017)	Controles de seguridad y privacidad para sistemas de información y organizaciones. Proporciona un catálogo de controles de seguridad y privacidad para sistemas de información y organizaciones para proteger las operaciones y activos de la organización, individuos, otras organizaciones y la nación de un conjunto diverso de amenazas que incluyen ataques hostiles, desastres naturales, fallas estructurales, errores humanos, y riesgos de privacidad.
TOGAF (The open group, 2018b)	Estándar de arquitectura empresarial, TOGAF, por sus siglas en inglés: The Open Group Architecture Framework. Un estándar de The Open Group. Es una metodología y un marco de arquitectura empresarial probado y utilizado por las organizaciones líderes en el mundo para mejorar la eficiencia del negocio.
OSSTMM 3 - The Open Source Security Testing methodology Manual V- 3 (ISECOM, 2010)	Es una metodología para probar la seguridad operativa de las ubicaciones físicas, las interacciones humanas y todas las formas de comunicación, como las inalámbricas, por cable, analógicas y digitales.

6. VOCABULARIO

Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 15 DE 19
		FECHA: 07/02/2019

Activo [Según ISO 27000]: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenaza [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. • **Análisis de Riesgo [Según ISO 27000]:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Auditoría [Según ISO 27000]: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria.

Autorización [Ley 1581 de 2012, art 3]: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Ciberseguridad [CONPES 3701]: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética.

Ciberspacio [Resolución CRC 2258 de 2009]: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.

Control [Según ISO 27000]: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos [Ley 1712 de 2014, art 6]: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Declaración de aplicabilidad [Según ISO 27000]: Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Framework: Marco de trabajo con lineamientos, conceptos y prácticas que sirve como referencia para tratar un tema específico.

Gestión de incidentes de seguridad de la información [Según ISO 27000]: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Impacto [Según ISO 27000]: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Información Pública Clasificada [Ley 1712 de 2014, art 6]: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 16 DE 19
		FECHA: 07/02/2019

Información Pública Reservada [Ley 1712 de 2014, art 6]: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos [Según ISO 27000]: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Riesgo [Según ISO 27000]: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo Residual [Según ISO 27000]: El riesgo que permanece tras el tratamiento del riesgo.

Seguridad de la información [Según ISO 27000]: Preservación de la confidencialidad, integridad, y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información SGSI [Según ISO 27000]: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua.

Vulnerabilidad [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

7. DESARROLLO

Para el diseño del plan de seguridad y privacidad de la información se toma como base el ciclo de mejora continua para lograr el desarrollo del Modelo de Seguridad y Privacidad de la Información teniendo en cuenta los siguientes aspectos:

7.1 Planeación

En esta fase se recopila la información de la fase preliminar y se determinan las actividades que deberán ser realizadas. En este sentido, actualmente la Entidad desde la Gerencia se ha comprometido y ha liderado junto con la Oficina de Sistemas de Información - TIC varias acciones que como resultado permitieron la elaboración, aprobación y adopción del Manual de políticas de seguridad de la información. Sin embargo, es fundamental la realización del autodiagnóstico para determinar el estado actual de la entidad, es necesario en esta fase definir actividades que apunten al logro de los objetivos propuestos del Modelo de Seguridad y Privacidad de la Información – MSPI relacionadas a continuación:

- Definir procedimientos de Seguridad de la Información.
- Definir guía de roles y responsabilidades de seguridad de la información.
- Realizar inventario y clasificación de activos de información, así como definir los responsables del levantamiento de este inventario por proceso.
- Desarrollar plan para la identificación, valoración y tratamiento de riesgos de seguridad de la información.
- Desarrollar plan de comunicaciones, uso y apropiación de las TIC.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 17 DE 19
		FECHA: 07/02/2019

- Realizar el autodiagnóstico de Seguridad y Privacidad de la Información de la Subred Integrada de Servicios de Salud Norte ESE utilizando la herramienta establecida por MINTIC, así mismo se tendrá en cuenta la matriz de autodiagnóstico de MIPG en lo referente a seguridad digital y gobierno digital.
- Realizar plan de transición IPV4 a IPV6

7.2 Hacer

En esta fase se lleva a cabo la implementación de la fase de planificación realizada, en donde es necesario sean ejecutadas las actividades descritas a continuación:

- Implementar del plan de tratamiento de riesgos de seguridad y privacidad de la información.
- Implementar controles de seguridad y privacidad de la información
- Establecer indicadores de gestión de la seguridad y privacidad de la información.
- Implementar el Cronograma del plan de transición de IPV4 a IPV6.
- Gestionar la respuesta a incidentes de seguridad de la información.

7.3 Verificar

En la fase de verificación de desempeño se realiza seguimiento y monitoreo al MSPI tomando como referencia los indicadores y métricas estratégicas, de gerencia y operativas que apoyen la posterior toma de decisiones sobre el MSPI por lo cual es necesario contemplar lo siguiente:

- Realizar plan de ejecución de auditorías, esta actividad se realizara acorde a lo definido por la oficina de Control Interno.
- Medir la efectividad de los controles y políticas definidas (Medición de los indicadores de gestión de la seguridad y privacidad de la información), se tendrán en cuenta la gestión de las incidencias de la mesa de servicios.
- Revisar los niveles de riesgos, esto se hará a través del cronograma de seguimiento a riesgos establecido por el proceso de Desarrollo Institucional.
- Actualizar si da a lugar los planes entorno a la seguridad de la información.

7.4 Actuar

En esta fase se consolidan los resultados de la fase anterior que sirven de insumo para elaborar el plan de mejoramiento continuo contemplando las acciones correctivas y preventivas adecuadas que contribuyan a la eficacia del MSPI, para lo cual es necesario realizar las siguientes actividades:

Desarrollar plan de mejora continua: Durante la vigencia del plan de seguridad y privacidad de la información se gestionaran las acciones correctivas y preventivas producto de los seguimientos y revisiones a la implementación y las auditorias programadas dentro del plan de auditoria de Control Interno.

Gestión de las comunicaciones, uso y apropiación de las TIC: La adecuada administración de las comunicaciones, uso y apropiación de las TIC permitirán fortalecer las estrategias para lograr una efectiva comunicación interna y externa de manera transversal, mejorando la gestión en temas de seguridad y privacidad de la información. La estrategia de comunicaciones, uso y apropiación de las

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 18 DE 19
		FECHA: 07/02/2019

TIC se traducirá en un plan de uso y apropiación de las TIC a ser ejecutado durante el período de duración del Plan de Seguridad y Privacidad de la Información; para ello se deberá tener en cuenta:

Mensaje y medios de comunicación: Los mensajes a transmitir se adecuarán a los distintos grupos que forman la audiencia, mediante comunicaciones escritas, página web, reuniones, comités, carteleras internas, intranet, videos y correos institucionales, Redes sociales y Boletines de la entidad.

8. SEGUIMIENTO Y MEDICIÓN

Como se mencionó en el punto 7.3 Verificar y 7.4 Actuar; el seguimiento, en este caso las auditorías internas se harán a través de la oficina de Control Interno de la Subred Integrada de Servicios de Salud Norte ESE y su medición será a través del cumplimiento del plan de mejoramiento que se tenga como resultado de estas auditorías.

9. BIBLIOGRAFÍA

Cartillas Guías sobre seguridad y privacidad de la información Alta Consejería TIC Distrital.
<http://ticbogota.gov.co/seguridad>

D-TI-25-Plan-Seguridad-Privacidad-Información de la Presidencia de la Republica de Colombia.

CONPES 3701 de 2011 Lineamientos de Políticas para Ciberseguridad y Ciberdefensa.

CONPES 3854 de 2016 Política Nacional de Seguridad Digital.

Documentación del Ministerio de Tecnología de la Información y comunicaciones MINTIC, articles-5482_Modelo_de_Seguridad_Privacidad.pdf.
<https://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02-02
		VERSIÓN : 2
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 19 DE 19
		FECHA: 07/02/2019

ANEXOS

- AP-GI-O-09-01 Documento Plan Estratégico de Tecnología de la información y Comunicaciones
- AP-GI-PL-04-01-Plan de Continuidad del Negocio
- AP-GI-PL-03-01 Plan de tratamiento del riesgo de la información

CONTROL DEL DOCUMENTO			
Versión	Fecha	Descripción de la modificación	Realizada por
1	19/10/2017	Creación	Nombre: Norberto Ruiz Rodríguez. Cargo: Jefe Oficina Sistemas de Información - TIC
2	07/02/2019	Se actualiza contenido en general en cumplimiento del acuerdo 642 de 2018	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			