

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 1 DE 50
		FECHA: 31/01/2024



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. 2024

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 2 DE 50
		FECHA: 31/01/2024

TABLA DE CONTENIDO

1	INTRODUCCIÓN	4
2	JUSTIFICACIÓN	4
3	ALCANCE	5
4	ENFOQUE DIFERENCIAL	5
5	OBJETIVOS	6
5.1	OBJETIVO GENERAL	6
5.2	OBJETIVOS ESPECIFICOS.....	6
6	MARCO NORMATIVO	6
7	VOCABULARIO	7
8	DESARROLLO.....	11
8.1	TALENTO HUMANO	11
8.1.1	Responsables de la implementación.....	11
8.1.2	Roles y responsabilidades	11
8.2	EQUIPOS BIOMÉDICOS.....	14
8.3	DISPOSITIVOS MÉDICOS E INSUMOS REQUERIDOS	14
8.4	METODOLOGÍA DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	14
8.4.1	Diagnostico.....	15
8.4.2	Planificación	17
8.4.3	Implementación	44
8.4.4	Evaluación de desempeño.....	44
8.4.5	Mejora continua	45
9	PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.....	45
10	SEGUIMIENTO Y MEDICIÓN	47
11	BIBLIOGRAFÍA	47
12	ANEXOS	48

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 3 DE 50
		FECHA: 31/01/2024

TABLA DE ILUSTRACIONES

Ilustración 1: Mapa de procesos institucional	5
Ilustración 2: Fases de implementación del modelo	14
Ilustración 3: Resultados autodiagnóstico MSPI 2023	16
Ilustración 4: Criterios de evaluación MSPI	16
Ilustración 5: Alineación Estratégica	17
Ilustración 6: Objetivos de Desarrollo Sostenible	19
Ilustración 7: Mapa de procesos institucional	28
Ilustración 8: Estructura orgánica institucional	39
Ilustración 9: Dimensión 3 MIPG, Fuente: Modulo 3 Gestión con valores para resultados	42
Ilustración 10: Proceso de gestión del riesgo en la seguridad de la información, Fuente: Norma Técnica Colombiana NTC-ISO/IEC 27005	43

TABLA DE TABLAS

Tabla 1: Roles y responsabilidades	14
Tabla 2: Evaluación de Controles	15
Tabla 3: Alineación Estratégica	18
Tabla 4: Plan de Desarrollo Nacional	20
Tabla 5: Alineación con Plan decenal de Salud Pública	21
Tabla 6: Plan de Desarrollo Distrital	22
Tabla 7: Alineación de los Planes Estratégicos	23
Tabla 8: Objetivos estratégicos Subred Norte	24
Tabla 9: Metas institucionales de la Subred Norte	26
Tabla 10: Tendencias Tecnológicas	27
Tabla 11: Procesos Estratégicos	28
Tabla 12: Procesos Misionales	29
Tabla 13: Procesos de Apoyo	29
Tabla 14: Procesos de Evaluación y Control Fuente:	29
Tabla 15: Alineación con los procesos Estratégicos	31
Tabla 16: Alineación con los procesos misionales	34
Tabla 17: Alineación con los procesos de apoyo	35
Tabla 18: Alineación con los procesos de evaluación y control	35
Tabla 19: Estándar de Gerencia de la Información	39
Tabla 20: Cronograma de trabajo del MSPI	45
Tabla 21: Indicador del plan de seguridad y privacidad de la información	47

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 4 DE 50
		FECHA: 31/01/2024

1 INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información es un documento que le permitirá a la Subred Integrada de Servicios de Salud Norte E.S.E. establecer los lineamientos y actividades para el diseño e implementación del Modelo de Seguridad y Privacidad de la Información, el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la Política de Gobierno Digital, arquitectura, servicios ciudadanos digitales y Seguridad de la Información.

La seguridad de la información no solo significa resguardar la información a través de copias de seguridad o en mecanismos de almacenamiento sofisticados o robustos, es decir que la tecnología no es el único factor que contribuye al aseguramiento. La Seguridad de la Información comprende una serie de planes, programas, metodologías, buenas prácticas, capacitación y sobre todo el compromiso de la alta dirección y de todo el personal involucrado con la finalidad de proteger la información que se genera y consume.

Dichos planes se deben mantener y mejorar de manera continua, tomado como base los riesgos que afectan a la seguridad de la información.

La implementación del Modelo de Seguridad y Privacidad de la Información ofrece la Subred Integrada de Servicios de Salud Norte E.S.E. beneficios económicos, legales y reputaciones como:

Reducción de los costos vinculados a los incidentes.

El incremento de los niveles de confianza de clientes.

Una mejora continua en la gestión de la seguridad.

Mejora y mantener la imagen de la organización.

Una garantía de continuidad y disponibilidad de los servicios informáticos.

Voluntad de cumplir con la legislación vigente de protección de datos de carácter personal, servicios de la sociedad de la información, comercio electrónico, propiedad intelectual.

Análisis de riesgos, identificando amenazas, vulnerabilidades e impactos en la organización.

Por lo anteriormente expuesto se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018 y contar con un instrumento guía para la ejecución de actividades que soporten la implementación de dicho Modelos de Seguridad y Privacidad de la Información – MSPI.

2 JUSTIFICACIÓN

De acuerdo con los últimos eventos presentados en Colombia relacionados con ciberseguridad, es importante para la Subred Integrada de Servicios de Salud Norte E.S.E. fortalecer de manera prioritaria las capacidades para enfrentar las amenazas a las cuales se ve expuesta, para ello se considera fundamental robustecer la visión tomando como referentes las mejores prácticas, fomentando la creación de una cultura de buen uso de las tecnologías y gestionando los riesgos de seguridad y privacidad de la información las cuales soportan las acciones para proteger los activos críticos de información, preservando su confidencialidad, integridad, disponibilidad y privacidad.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 5 DE 50
			FECHA: 31/01/2024

3 ALCANCE

Teniendo en cuenta la estructura el mapa de procesos de la Subred Integrada de Servicios de Salud Norte ESE, el plan de seguridad y privacidad de la información aplica para todos los procesos por su nivel de sensibilidad ya que su daño o pérdida, pueden llevar un impacto negativo de índole legal, operativa, de imagen o económica para la entidad.



Ilustración 1: Mapa de procesos institucional

Teniendo en cuenta el análisis de contexto, el alcance del SGSI- MSPI, de acuerdo con las características de la entidad, su ubicación y sus activos de información; la Subred Integrada de Servicios de Salud Norte E.S.E implementa y opera el SGSI- MSPI en términos del modelo PHVA (Planear, Hacer, Verificar y Actuar), para los activos clasificados como información pública reservada de los procesos misionales (Gestión Ambulatoria, Urgencias, Hospitalización y Cirugía) y de apoyo (Gestión Financiera, Información y TICS), que componen el mapa de procesos de la entidad. De la misma manera; la Subred Integrada de Servicios de Salud Norte E.S.E, determinara los controles de acuerdo con lo establecido en el Anexo A de la norma NTC/ISO 27001:2013.

4 ENFOQUE DIFERENCIAL

El prestador de servicios de salud cuenta con información documentada de las actividades y procedimientos que se realizan en el servicio acordes con su objeto, alcance y enfoque diferencial mediante guías de práctica clínica- GPC, procedimientos de atención, protocolos de atención y otros documentos que el prestador de servicios de salud determine, dicha información incluye talento humano, equipos biomédicos, medicamentos y dispositivos médicos e insumos requeridos. CRITERIO DE RESOLUCIÓN 3100 DE 2019 - PAGINA 73 PUNTO 6

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 6 DE 50
		FECHA: 31/01/2024

5 OBJETIVOS

5.1 OBJETIVO GENERAL

Definir las actividades del Plan la Seguridad y Privacidad de la Información de la Subred Integrada de Servicios de Salud Norte ESE, por medio de los lineamientos establecidos el ciclo PHVA definido en la norma ISO 27001, el modelo de referencia definido por el Ministerio de Tecnologías de Información, la Política de Gobierno Digital y plataforma estratégica de la Subred Integrada de Servicios de Salud Norte E.S.E, de acuerdo con el modelo del Sistema de Gestión de Seguridad de la Información, con el fin de consolidar la operación y contribuir al logro de los objetivos y requisitos normativos en materia de la Modelo de Seguridad y Privacidad de la Información - MSPI y el Modelo Integrado de Planeación y Gestión (MIPG).

5.2 OBJETIVOS ESPECIFICOS

- Administrar y proteger los activos de información de la Subred Integrada de Servicios de Salud Norte E.S.E, teniendo en cuenta los criterios de confidencialidad, integridad y disponibilidad.
- Realizar campañas de sensibilización a todos los colaboradores de la Subred Integrada de Servicios de Salud Norte E.S.E del MSPI (Modelo de Seguridad y Privacidad de la Información).
- Realizar el monitoreo de la infraestructura de TI mediante herramientas que permitan tener una visión en tiempo real de su estado y las vulnerabilidades de los equipos para prevenir posibles ataques informáticos.
- Implementar acciones mejora para el MSPI y el MIPG de acuerdo con lo establecido en la política de Gobierno Digital. Administrar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.

6 MARCO NORMATIVO

Para el diseño del plan de seguridad de la información la Subred Integrada de Servicios de Salud Norte E.S.E toma como referencia:

- El Modelo de Seguridad y Privacidad de la Información de MINTIC
- Norma NTC-ISO/IEC: 27001 - 2013
- Decreto 103 de 2015 el cual reglamenta parcialmente la ley 1712 de 2014 "Ley de Transparencia "
- Ley 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013 y por el Decreto 1081 de 2015, "Protección de datos personales".
- Decreto único reglamentario 1078 de 2015 – MinTIC – Modelo de Seguridad y Privacidad de Información.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 7 DE 50
		FECHA: 31/01/2024

- Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones – TIC Se crea la agencia Nacional de espectro y se dictan otras disposiciones.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Anexo 4 Lineamientos para la Gestión del Riesgo de Seguridad Digital en Entidades Públicas - Guía riesgos 2018 La anterior documentación ofrece un enfoque para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información (SGSI) a través del modelo (PHVA)
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.
- Decreto 338 de 2022. Se establecen lineamientos generales para fortalecer la gobernanza de seguridad digital, se crea el modelo y las instancias de gobernanza de seguridad digital y se dictan otras disposiciones.

7 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).

Activo: 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 tengavalor para la organización. (ISO/IEC 27000).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controlar en su calidad de tal.

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).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema oa la organización. (ISO/IEC 27000).

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 8 DE 50
		FECHA: 31/01/2024

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

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

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

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

Ciberespacio: 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. (Resolución CRC 2258 de 2009).

Control: 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: 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 (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: 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. (Decreto 1377 de 2013, art 3).

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Mixtos: Para efectos de esta guía es la información que contiene datos personales

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 9 DE 50
		FECHA: 31/01/2024

públicos junto con datos privados o sensibles.

Datos Personales 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. (Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad: 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. (ISO/IEC 27000).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: 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. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

Información Pública Clasificada: 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. (Ley 1712 de 2014, art 6).

Información Pública Reservada: 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. (Ley 1712 de 2014, art 6).

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 recuperación de desastres – DRP: La recuperación de desastres es un proceso mediante el cual una organización anticipa y aborda desastres relacionados con la tecnología. Los sistemas de TI de cualquier compañía pueden sufrir una interrupción de manera inesperada debido a circunstancias imprevistas, como cortes de energía, fenómenos naturales o errores de seguridad. La recuperación de desastres incluye los

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 10 DE 50
		FECHA: 31/01/2024

procedimientos y políticas de una compañía para recuperarse con rapidez de tales eventos.

El DRP es un componente del Plan de Continuidad de Negocio (BCP) de la organización, y del mismo modo debe ser probado y actualizado regularmente para asegurar que el equipo de TI pueda tener éxito en los esfuerzos de recuperación independientemente del tipo de desastre.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.(ISO/IEC 27000).

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsabilidad Demostrada: Conducta desplegada por los responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

Responsable del Tratamiento de Datos: 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. (Ley 1581 de 2012, art 3).

Riesgo: 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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: 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. (ISO/IEC 27000).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 11 DE 50
		FECHA: 31/01/2024

8 DESARROLLO

8.1 TALENTO HUMANO

8.1.1 Responsables de la implementación

El plan de Seguridad y Privacidad de la Información de acuerdo con los requisitos de la norma ISO 27001-2013, requiere de una participación activa y comprometida de la alta dirección y será gestionado por los servidores públicos y/o contratistas asignados por la gerencia. Por lo tanto, la Alta Dirección liderará y apoyará la implementación del MSPI (Modelo de Seguridad y Privacidad de Información), para lo cual establecerá la estructura funcional y las competencias de los organismos y/o el equipo requerido para la implementación y mantenimiento del SGSI-MSPI, como se muestra a continuación:

8.1.2 Roles y responsabilidades

ROL	ACTIVIDADES	RESPONSABILIDADES
Alta Dirección	Coordinar, dirigir y orientar la planeación, implementación, evaluación y mejoramiento del MSPI.	Coordinar la implementación del MSPI al interior de la Subred Integrada de Servicios de Salud Norte ESE. Revisar los diagnósticos efectuados a la seguridad de la información de la Subred Integrada de Servicios de Salud Norte ESE, de acuerdo con lo estipulado por la norma. Apoyar el desarrollo de proyectos relacionados con seguridad. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. Promover la difusión y sensibilización de la seguridad de la información en la Subred Integrada de Servicios de Salud Norte E.S.E.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 12 DE 50
		FECHA: 31/01/2024

ROL	ACTIVIDADES	RESPONSABILIDADES
Comité Institucional de Gestión y Desempeño	Dirigir y orientar la planeación, implementación y mejoramiento del MSPI. Coordinar la evaluación del desempeño del MSPI. Velar por el cumplimiento de las políticas de seguridad de la información.	Facilitar la administración y desarrollo de iniciativas sobre seguridad de información en la entidad. Revisar y aprobar los lineamientos establecidos en pro de asegurar que la información se encuentre protegida, garantizando la confidencialidad, la integridad y la disponibilidad de la información y de los recursos informáticos que la soportan. Revisar y analizar los incidentes de seguridad considerados como de alto impacto o severos reportados en la Subred Integrada de Servicios de Salud Norte ESE. Identificar necesidades de evaluación de procesos soportados por recursos informáticos y su plataforma tecnológica. Avalar y aprobar la ejecución de proyectos de seguridad de información. Validar y aprobar las Políticas de Seguridad de Información o las modificaciones a las mismas. Definir roles y responsabilidades específicos que se relacionen con la seguridad de la información. Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. Evaluar planes de acción para mitigar y/o eliminar riesgos.
Oficial de Seguridad de la Información.	Propender por el cumplimiento de las políticas de seguridad de la información de la Subred Integrada de Servicios de Salud Norte ESE	Aplicar y promover metodologías y estándares que conduzcan a la práctica de una cultura de la información. Gestionar la aplicación de las políticas de seguridad de la información. Diseñar estrategias que puedan garantizar la seguridad de los recursos informáticos Evaluar la implementación de controles específicos de seguridad de la información. Supervisar el cumplimiento de los principios básicos de seguridad de la información (Confidencialidad, Integridad y Disponibilidad). Brindar asesoría a las demás áreas en el proceso de implementación de controles de seguridad.
Responsable de Seguridad de la Información o a quien se delegue.	Planear, ejecutar, verificar y realizar seguimiento a la implementación del MPSI	Socializar documentación generada en el comité de gestión institucional, relacionada con seguridad de la información y que impacten a la Subred Integrada de Servicios de Salud Norte ESE. Identificar la brecha entre el MSPI y la situación actual de la Subred Norte ESE. Generar y hacer seguimiento al cronograma del plan de implementación del MSPI. Gestionar el equipo de seguridad de la información, definiendo roles, responsabilidades, entregables y tiempos. Realizar un seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos del MSPI, para su solución oportuna y escalar al comité de gestión institucional en caso de ser necesario. Velar por el mantenimiento de la documentación del MSPI. Liderar la implementación del MSPI al interior de la Subred

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 13 DE 50
		FECHA: 31/01/2024

ROL	ACTIVIDADES	RESPONSABILIDADES
		Integrada de Servicios de Salud Norte ESE y realizar la medición a través de los indicadores de gestión definidos para tal fin.
Jefe Oficina Desarrollo Institucional	Coordinar la implementación del MSPI en la Subred Integrada de Servicios de Salud Norte ESE, garantizando su integración al SIG. Establecer los lineamientos necesarios para proteger la información de datos personales generados y custodiados.	Garantizar la articulación del sistema al Sistema Integrado de Gestión. Velar porque se eviten la generación de riesgos de Seguridad de la Información. Definir e implementar políticas de protección de datos y privacidad de información sensible de acuerdo a los requerimientos legales establecidos.
Jefe Oficina de Sistemas de Información TIC.	Velar por el cumplimiento de las políticas de seguridad de la información establecidas. Velar por el cumplimiento de las políticas de seguridad de la información establecidas para la infraestructura tecnológica.	Establecer controles de seguridad de la información en los procesos relacionados con Gestión de la Información, con el fin de prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información y servicios que presta la Oficina de Sistemas de la Información TIC. Establecer controles de seguridad informática en la infraestructura tecnológica de la Subred Integrada de Servicios de Salud Norte ESE en: Equipos de Cómputo, Servidores, Elementos de Redes y Comunicaciones. Prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información de la infraestructura tecnológica.
Subgerencia Corporativa	Asignar los recursos necesarios para garantizar la seguridad física de las instalaciones y la información de la Subred Integrada de Servicios de Salud Norte E.S.E.	Garantizar los recursos para la implementación de los controles operacionales con el fin de evitar riesgos que afecten la seguridad de la información de la Subred Integrada de Servicios de Salud Norte ESE.
Jefe Oficina Asesora Jurídica	Identificar y mantener actualizado el normograma de seguridad.	Identificar los aspectos legales en referencia a la Seguridad de la Información.
Director de Talento Humano	Evaluar la competencia del Talento Humano en el cumplimiento del MSPI, así como la implementación de programas de conciencia y sensibilización del sistema.	Garantizar la capacitación y competencia del Talento Humano que preste sus servicios para la Subred Integrada de Servicios de Salud Norte ESE o que actúe en nombre del mismo en el Sistema de Gestión de Seguridad de la Información.
Responsable de Gestión Documental	Garantizar la seguridad de la información en el archivo.	Establecer controles de seguridad de la información con el fin de prevenir riesgos que puedan afectar la confidencialidad, disponibilidad e integridad de la información almacenada en el Archivo.
Responsable Oficina de Control Interno	Planear y realizar las auditorías integrales al SG	Revisar el cumplimiento de los requisitos de la norma en el Sistema de Gestión de Seguridad de la Información de la Subred Integrada de Servicios de Salud Norte ESE y evidenciar mejoras del mismo.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 14 DE 50
		FECHA: 31/01/2024

ROL	ACTIVIDADES	RESPONSABILIDADES
Funcionarios y Contratistas de la Subred Integrada de Servicios de Salud Norte ESE.	Dar cumplimiento a las disposiciones establecidas por la Subred Integrada de Servicios de Salud Norte ESE en materia de políticas de seguridad de la información.	Garantizar la confidencialidad respecto de la información que reciben, generan y procesan durante el desarrollo de sus actividades en la Subred Integrada de Servicios de Salud Norte E.S.E. No transmitir, publicar o difundir información como datos personales, para ser usados para finalidades diferentes por la que hayan sido recogidos. Comunicar al responsable de seguridad de la información del de cualquier incidencia respecto a la seguridad de la información. Solicitar autorización escrita para la recolección de información personal, con carácter institucional. Mantener la confidencialidad, integridad y disponibilidad de la información. Hacer un buen uso de los activos de información de la Entidad. Aplicar los controles que sean identificados a su cargo para minimizar los riesgos que fueron identificados

Tabla 1: Roles y responsabilidades

8.2 EQUIPOS BIOMÉDICOS

Aplica según necesidades y estudios de investigación

8.3 DISPOSITIVOS MÉDICOS E INSUMOS REQUERIDOS

No aplica

8.4 METODOLOGÍA DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El presente Plan de Seguridad y Privacidad de la Información, se estructura de acuerdo a la ISO 27001:2013 y el anexo A, el cual hace parte integral del presente plan y establece cada una de las actividades y compromisos a ejecutar durante la vigencia del presente documento.

El modelo en el que se basa el Sistema de Gestión de Seguridad de la Información - SGSI se denomina PHVA (Planear-Hacer-Verificar- Actuar), con una fase previa de diagnóstico. La siguiente figura ejemplifica las fases de implementación del modelo.

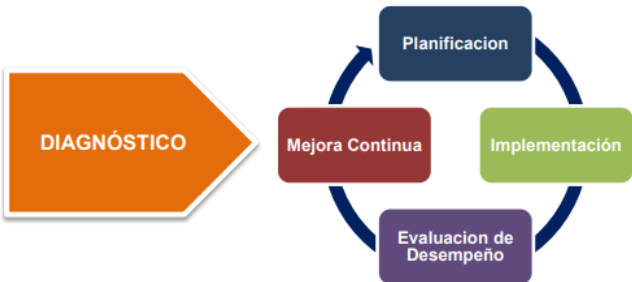


Ilustración 2:Fases de implementación del modelo

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 15 DE 50
		FECHA: 31/01/2024

Fuente: Lineamientos para la Implementación del Modelo de Seguridad de la Información Ministerio de Tecnologías de la Información y las Comunicaciones.

8.4.1 Diagnóstico

Esta etapa se inicia con el análisis de brechas GAP de seguridad de la información, el cual se refiere al espacio entre "donde estamos" (el presente) y "donde queremos estar" (el objetivo a alcanzar). El GAP es la auditoría inicial que nos permite:

- Establecer el punto de partida
- Determinar el grado de implantación del modelo
- Evaluar el avance del proyecto
- Determinar los recursos necesarios para alcanzar los objetivos, y
- Determinar el alcance del MSPI y la política de seguridad.

Para el análisis de brecha se tuvo en cuenta:

- Revisión del cumplimiento de las exigencias de la Norma ISO 27001
- Identificar requisitos faltantes (Políticas, procedimientos, controles), los cuales son exigidos por la norma ISO 27001 y por los modelos del MinTic – MSPI.

De acuerdo con lo establecido por MINTIC, la Subred Integrada de Servicios de Salud Norte E.S.E utilizará la herramienta de auto diagnóstico de seguridad y privacidad de la información, la cual nos permite establecer el estado de los diferentes dominios de la norma y determinar el grado de madurez del MSPI.

Al aplicar la herramienta con corte a noviembre de 2023, se obtienen los siguientes resultados:

No.	Evaluación de Efectividad de controles			EVALUACIÓN DE EFECTIVIDAD DE CONTROL
	DOMINIO	Calificación Actual	Calificación Objetivo	
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	70	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	58	100	EFFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	33	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	64	100	GESTIONADO
A.9	CONTROL DE ACCESO	61	100	GESTIONADO
A.10	CRİPTOGRAFÍA	0	100	İNEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	55	100	EFFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	49	100	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	75	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	29	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	60	100	EFFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	37	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	67	100	GESTIONADO
A.18	CUMPLIMIENTO	45	100	EFFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		50	100	EFFECTIVO

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 16 DE 50
		FECHA: 31/01/2024

Tabla 2: Evaluación de Controles
Fuente: Autodiagnóstico MSPI con corte a noviembre de 2023

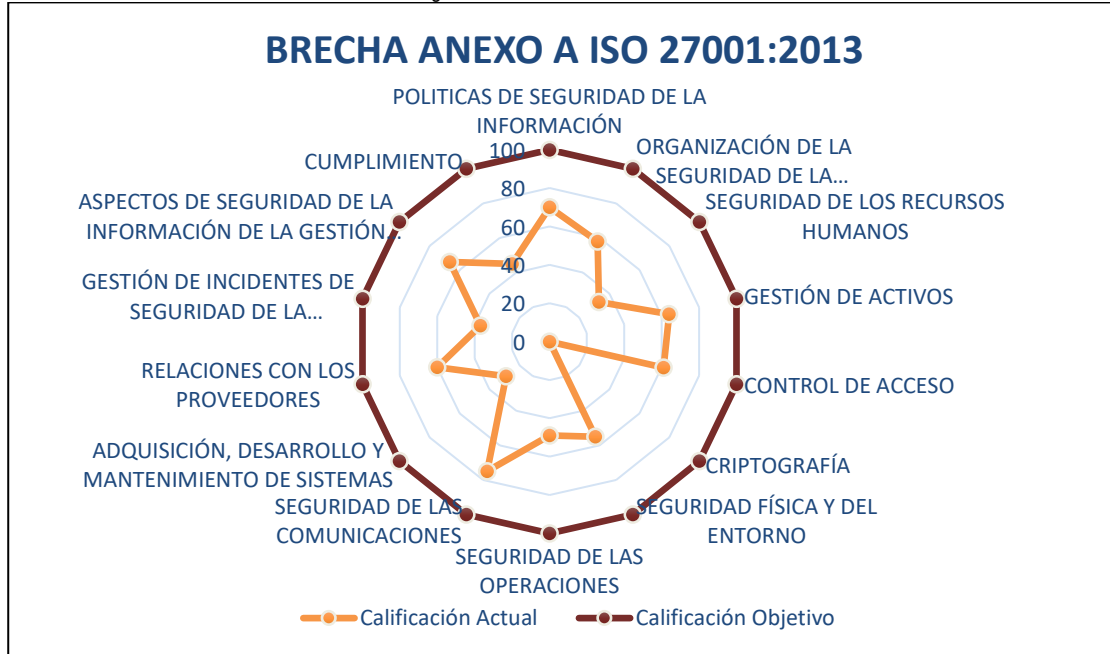


Ilustración 3: Resultados autodiagnóstico MSPI 2023
Fuente: Autodiagnóstico MSPI con corte a noviembre de 2023

Los dominios evaluados se encuentran en estados:

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuentan con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo.

Ilustración 4: Criterios de evaluación MSPI
Fuente: Autodiagnóstico MSPI con corte a noviembre de 2023

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 17 DE 50
			FECHA: 31/01/2024

8.4.2 Planificación

Con los resultados de la anterior fase, la plataforma estratégica de la Subred Integrada de Servicios de Salud Norte E.S.E y la metodología de gestión del riesgo de MinTIC, es posible definir el alcance del MSPI con un enfoque por procesos y extendido a toda la Subred.

8.4.2.1 Identificación del Contexto

Esta fase consiste en identificar en qué medida los aspectos internos y externos podrían afectar al propósito de la organización y a su capacidad para lograr los resultados esperados del MSPI. En este sentido, se debe entender como la Subred Integrada de Servicios de Salud Norte E.S.E apoyada en su plataforma estratégica. Lo anterior requiere comprender los procesos y procedimientos en los que se soporta para cumplir los objetivos, determinar el contexto interno y externo, definir la relación con cada una de las partes interesadas, es decir, todas aquellas personas u organizaciones que pueden influir o verse afectadas por la falta de seguridad de la información en la Subred.

Contexto externo - Motivadores estratégicos.

Esta sección del documento hace referencia a la identificación de los motivadores estratégicos a nivel Nación, a Nivel territorio, a nivel entidad y los lineamientos y Políticas que dan línea en la orientación y alineación la Estrategia de Tecnologías de la Información (PETI) de las entidades del País.

Alineación estratégica



Ilustración 5: Alineación Estratégica
Fuente: Plan estratégico de tecnologías de la información - PETI

Motivador	Fuente
Estrategia Nacional	- Objetivos de Desarrollo Sostenible - Plan Nacional de Desarrollo - Pacto por la Transformación Digital

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 18 DE 50
		FECHA: 31/01/2024

Motivador	Fuente
Estrategia Sectorial	- Plan decenal de Salud pública - Plan de Desarrollo Distrital
Estrategia Institucional	- Plan Operativo Anual
Lineamientos y Políticas	- Transformación Digital - Política de Gobierno Digital - Modelo Integrado de Planeación y Gestión.

Tabla 3: Alineación Estratégica

Fuente: Plan estratégico de tecnologías de la información - PETI

Objetivos de Desarrollo Sostenible

En septiembre de 2015, más de 150 jefes de Estado y de Gobierno se reunieron en la histórica Cumbre del Desarrollo Sostenible en la que aprobaron la Agenda 2030. Esta Agenda contiene 17 objetivos de aplicación universal que, desde el 1 de enero de 2016, rigen los esfuerzos de los países para lograr un mundo sostenible en el año 2030.

Los Objetivos de Desarrollo Sostenible (ODS) son herederos de los Objetivos de Desarrollo del Milenio (ODM) y buscan ampliar los éxitos alcanzados con ellos, así como lograr aquellas metas que no fueron conseguidas.

Estos nuevos objetivos presentan la singularidad de instar a todos los países, ya sean ricos, pobres o de ingresos medianos, a adoptar medidas para promover la prosperidad al tiempo que protegen el planeta. Reconocen que las iniciativas para acabar con la pobreza deben ir de la mano de estrategias que favorezcan el crecimiento económico y aborden una serie de necesidades sociales, entre las que cabe señalar la educación, la salud, la protección social y las oportunidades de empleo, a la vez que luchan contra el cambio climático y promueven la protección del medio ambiente.

A pesar de que los ODS no son jurídicamente obligatorios, se espera que los gobiernos los adopten como propios y establezcan marcos nacionales para su logro. Los países tienen la responsabilidad primordial del seguimiento y examen de los progresos conseguidos en el cumplimiento de los objetivos, para lo cual es necesario recopilar datos fiables, accesibles y oportunos. Las actividades regionales de seguimiento y examen se basarán en análisis llevados a cabo a nivel nacional y contribuirán al seguimiento y examen a nivel mundial.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 19 DE 50
		FECHA: 31/01/2024

Se establecieron 17 Objetivos, los cuales se describen a continuación:



Ilustración 6: Objetivos de Desarrollo Sostenible
Fuente: Plan estratégico de tecnologías de la información - PETI

Desde hace tiempo se reconoce que para conseguir una economía robusta se necesitan inversiones en infraestructura. Las inversiones en infraestructura (transporte, energía, comunicaciones, etc.) son fundamentales para lograr un desarrollo sostenible, empoderar a las sociedades de numerosos países, fomentar una mayor estabilidad social y conseguir ciudades más resistentes al cambio climático.

Además de los fondos gubernamentales y de la asistencia oficial para el desarrollo, también se está promoviendo la inversión del sector privado para los países que necesitan recursos financieros y tecnológicos.

El Objetivo 9 busca Construir infraestructuras resilientes, promover la industrialización inclusiva y sostenible y fomentar la innovación; contemplando en una de sus metas:

Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020.

Plan de Desarrollo de la Nación

En el libro 1 /Numeral 2/ Objetivos y estrategias del Plan Nacional de Desarrollo 2018-2022 Pacto por Colombia, pacto por la equidad, Pactos transversales: VII. Pacto por la transformación digital de Colombia: Gobierno, empresas y hogares conectados con la era del conocimiento.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 20 DE 50
		FECHA: 31/01/2024

OBJETIVO	NUMERAL	ITEM
Objetivo 3. Articular todos los agentes del sector salud en torno a la calidad	e) Incentivar herramientas que pongan a disposición información de calidad y desempeño de cara a los usuarios para empoderarlos en la toma de decisiones	• MINSALUD promoverá la modernización de la gestión de prestación de servicios a través de avances en la interoperabilidad de los sistemas de información y mejoras en conectividad en los territorios apartados, en articulación con los lineamientos de MinTIC (impulsando los programas de telesalud, historia clínica electrónica interoperable, factura electrónica y demás apropiaciones TIC) y en el marco de los Servicios Ciudadanos Digitales. • Se desarrollará el marco jurídico que asegure el flujo de información dentro del Sistema de Seguridad Social Integral, para garantizar la prestación de los servicios asociados al mismo, armonizando la normatividad relativa a la política nacional de explotación de datos, protección de datos personales y seguridad digital que rigen la materia.
	f) Incentivar la investigación en salud	• Se promoverán y apoyarán proyectos que aporten a la innovación, investigación y desarrollo en prestación de servicios; o modelos de salud que apuesten a la transformación tecnológica del sector, en articulación con los lineamientos de MinTIC y en el marco de los Servicios Ciudadanos Digitales.
4) Objetivo 4. Lograr más infraestructura y dotación en salud, como soporte al acceso efectivo y localidad	a) Instituciones prestadoras de servicios de salud dotadas con infraestructura adecuada y capacidad para responder con calidad y efectividad a las necesidades de toda la población	• Se implementará un plan de acción inmediato para los hospitales públicos, con el fin de identificar las necesidades en infraestructura, dotación, calidad, talento humano y sostenibilidad. Se aplicará un modelo diferencial de acuerdo con las necesidades identificadas y la priorización que defina Min Salud.

Tabla 4: Plan de Desarrollo Nacional
Fuente: Plan estratégico de tecnologías de la información - PETI

Plan Decenal de Salud

En el Plan Decenal de Salud Pública PDSP 2012-2021 se plantea la línea de trabajo para dar respuesta a los desafíos actuales en salud pública y para consolidar, en el marco del sistema de protección social, Las capacidades técnicas en los ámbitos nacional y territorial para la planeación, ejecución, seguimiento Evaluación de las intervenciones, de acuerdo con los Objetivos de Desarrollo del Milenio (ONU,2000).

DIMENSIONES GENERALES	DIMENSIÓN ESPECÍFICA	COMPONENTE
	2. Vida saludable y condiciones no transmisibles	b. Condiciones crónicas prevalentes: tecnologías apropiadas para la promoción y la atención integral.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 21 DE 50
		FECHA: 31/01/2024

DIMENSIONES GENERALES	DIMENSIÓN ESPECÍFICA	COMPONENTE
Dimensiones prioritarias	3. Convivencia social y salud mental	a. Promoción de la salud mental y la convivencia: uso de tecnologías de la información y las comunicaciones en pro de la salud mental.
	5. Sexualidad, derechos sexuales y reproductivos	b. Prevención y atención integral en salud sexual reproductiva desde un enfoque de derechos: abordaje integral de las violencias de género y violencias sexuales, que incluye consolidación de sistemas de información, gestión articulada entre programas e instituciones y atención integral a víctimas.
Dimensiones transversales	1P5/1. Gestión diferencial de poblaciones vulnerables	a. Componente: Desarrollo integral de las niñas, niños y adolescentes: gerencia de las políticas públicas de primera infancia, infancia y adolescencia; estrategias de disminución de barreras de acceso a los servicios de salud; estrategias de tecnologías de la información y las comunicaciones al servicio de la salud. e. Componente: Discapacidad: articulación y gestión intersectorial para el acceso de la población con discapacidad al ámbito educativo, laboral, social, cultural, de participación ciudadana, a las tecnologías de la información y las comunicaciones.

Tabla 5: Alineación con Plan decenal de Salud Pública
Fuente: Plan estratégico de tecnologías de la información - PETI

Plan de Desarrollo Distrital

Plan de Desarrollo Distrital 2020-2024 “Un Nuevo Contrato Social y Ambiental Para El Siglo XXI”; dentro de su estructura contiene en Artículo 13. Dentro de su estructura tiene 5 propósitos, 30 logros de la ciudad y 70 programas generales.

PROPÓSITO	LOGRO DE LA CIUDAD	PROGRAMA	ITEM
Propósito 1: Hacer un nuevo contrato social con igualdad de oportunidades para la inclusión social, productiva y política.	Completarla implementación de un modelo de salud con enfoque poblacional- diferencial, de género, participativo, resolutorio y territorial que aporte a la modificación de los determinantes sociales de la salud.	Mejora de la gestión de instituciones de salud.	2024 cumplir con el 100% en la implementación de la arquitectura empresarial de soluciones que integran exitosamente la mejora de los procesos estratégicos, técnicos y operativos de la Dirección Territorial de Salud. A 2024 el sector salud contará con una infraestructura y dotación que le permita prestar servicios con calidad y oportunidad acorde con el Modelo de Salud basado en el enfoque poblacional, diferencial, participativo, resolutorio y territorial.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 22 DE 50
			FECHA: 31/01/2024

PROPÓSITO	LOGRO DE LA CIUDAD	PROGRAMA	ITEM
			A 2024 mantener por encima del 95% la interoperabilidad de la Historia Clínica Electrónica en las 4 subredes de servicios de salud y avanzar en los puntos de la redprivada priorizados.
Propósito 5: Construir Bogotá Región con gobierno abierto, transparente y ciudadanía Consciente.	Posicionar al Gobierno Abierto de Bogotá-GABO como una nueva forma de gobernanza que reduce el riesgo de corrupción e incrementa el control ciudadano del Gobierno	Gobierno Abierto	A 2024, diseñar e implementar la Estrategia de Gobierno Abierto en salud de Bogotá D.C. (GABO), a través de acciones de participación social en salud, transparencia, control social y rendición de cuentas.
	Posicionar globalmente a Bogotá como territorio inteligente (Smart City)	Transformación digital y gestión de TIC para un territorio inteligente	A 2024 diseñar e implementar la Estrategia de Transformación Digital en Salud

Tabla 6: Plan de Desarrollo Distrital.
 Fuente: Plan estratégico de tecnologías de lainformación - PETI

Alineación Planes Estratégicos

	ESTRATEGIA NACIONAL	ESTRATEGIA SECTORIA	DISTRITAL	INSTITUCIONAL
	Min Salud promoverá la modernización de lagestión de prestación de servicios a través de avances en la interoperabilidad de los sistemas de información y mejoras en conectividad en los territorios apartados, en articulación con los lineamientos de MinTIC (impulsando los programas de telesalud, historia clínica electrónica interoperable, factura electrónica y demás apropiaciones TIC) y en el marco de los Servicios Ciudadanos Digitales.	b. Prevención y atención integral en salud sexual reproductiva desdeun enfoque de derechos: abordajeintegral de lasviolencias de géneroy violencias sexuales, queincluye consolidación de sistemas de información, gestión articulada entre programas e instituciones yatención integral avíctimas.	A 2024 mantener por encima del 95% la interoperabilidad de la Historia Clínica Electrónica en las 4 subredes de servicios de salud y avanzar en los puntos de la red privada priorizados.	Implementar el Módulo de Inteligencia de negocios del sistema de información Servinte Clinical Suite acorde con un plan de trabajo.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 23 DE 50
		FECHA: 31/01/2024

	ESTRATEGIA NACIONAL	ESTRATEGIA SECTORIA	DISTRITAL	INSTITUCIONAL
	Se implementará un plan de acción inmediato para los hospitales públicos, con el fin de identificar las necesidades en infraestructura, dotación, calidad, talento humano y sostenibilidad. Se aplicará un modelo diferencial de acuerdo con las necesidades identificadas y la priorización que defina MinSalud	b. Condiciones crónicas prevalentes: tecnologías apropiadas para la promoción y la atención integral	A 2024 el sector salud contará con una infraestructura y dotación que le permita prestar servicios con calidad y oportunidad acorde con el Modelo de Salud basado en el enfoque poblacional, diferencial, participativo, resolutivo y territorial.	

Tabla 7: Alineación de los Planes Estratégicos
Fuente: Plan estratégico de tecnologías de la información - PETI

Contexto Institucional

Misión

Somos una Empresa Social del Estado innovadora y socialmente responsable, que presta servicios de salud integrales y de calidad, con participación activa en la formación de talento humano y desarrollo de la docencia y la investigación, contribuyendo al mejoramiento de la calidad de vida de la población

Visión

Para el 2030, la Subred Integrada de Servicios de Salud Norte E.S.E será reconocida como la Empresa Social del Estado, líder en la prestación de servicios asistenciales de excelencia, centrada en la persona, con atención humanizada, a través de la formación del recurso humano asistencial y administrativo de alta calidad, inspirada por la investigación y el desarrollo. Tendremos un modelo de gestión económico, ambientalmente sostenible, generador de equidad y legitimidad social.

Objetivos Estratégicos

ID	Objetivo
	A. MODERNIZACIÓN EMPRESARIAL DE LA SUBRED NORTE E.S.E. PERSPECTIVA
001	Fortalecer la línea de gestión empresarial operacional - Productividad
002	Desarrollar línea de gestión institucional - Competitividad
003	Desarrollar línea de gestión ambiental - Sostenibilidad
	B. PERSPECTIVA FINANCIERA
004	Lograr la sostenibilidad financiera de la Subred Norte

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 24 DE 50
		FECHA: 31/01/2024

ID	Objetivo
	C. PERSPECTIVA CLIENTES
005	Incrementar nivel de fidelización y satisfacción de los usuarios
006	Desarrollar línea de gestión social - Legitimidad
007	Diversificación portafolio de servicios
008	Incrementar portafolio de clientes
	D. PERSPECTIVA PROCESOS
009	Alcanzar estándares superiores de calidad en salud
010	Implementar sistemas integrales de gestión en la Subred Norte
	E. PERSPECTIVA DE INNOVACIÓN Y APRENDIZAJE
011	Generar y difundir crecimiento científico en salud
012	Fortalecer competencias del Talento Humano con énfasis en docentes y estudiantes
013	Fortalecer el sistema de información y comunicaciones

Tabla 8: Objetivos estratégicos Subred Norte
Fuente: Plan estratégico de tecnologías de la información - PETI

Indicadores plan de desarrollo institucional

ID	META	LÍNEA BASE
001	Implementar al 100% el aplicativo de semaforización incluidos los indicadores trazadores (PDD)	No Existe
002	Ejecutar al 100% un programa de atención a brotes en salud pública. (PDD)	Covid-19
003	Desplegar una estrategia a través de equipos interdisciplinarios para el abordaje del 100% de las acciones PSPIC. (PTS)	Existe por PSPIC
004	Mejorar los indicadores trazadores en un 1%, para optimizar la capacidad instalada mejorando la producción de los servicios asistenciales, hospitalarios, ambulatorios, complementarios, urgencias y de gestión del riesgo. (DF)	Existe por servicios
005	Incrementar la contratación de servicios de salud a través de la EAPB así (DF): - Unidad ejecutora o Funcional Unidad de quemados 41.799.493.419 - Continuidad de la Unidad ejecutora APH, el costo fue proyectado 60.901.311.870 - Incrementar la oferta de servicios de grupos quirúrgicos del 5% para todos los pagadores 3.887.816.976	Existe histórico de contratación
006	Implementar el 100% de las RIAS priorizadas (PTS)	9 RIAS
007	Implementar al 100% la automatización del laboratorio en la UMHEs Simón Bolívar y la puesta en marcha del laboratorio de biología molecular en la UMHEs calle 80, buscando mejorar los tiempos de operación con miras a la mejora de la oportunidad.	No Existe
008	Cumplir al 100% con los proyectos inscritos en el Plan Bienal de Inversión y aprobados por la SDS (infraestructura y dotación). (PDD)	9 proyectos inscritos en BPIN

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 25 DE 50
		FECHA: 31/01/2024

ID	META	LÍNEA BASE
009	Ejecutar en un 80% el PINAR (incluye disminuir en 90% el consumo de papel en los servicios asistenciales y administrativos).	porcentaje de ejecución: 74%
010	Implementar al 25% el hospital verde en la Subred Norte (PDD)	Existe por unidad
011	Recaudar sobre la facturación de la vigencia por año, ascendente así (DF): 2020 72%; 2021 76%; 2022 80%; 2023 86%. Aplica para cada vigencia IPC +2% vía tarifa	Informe de gestión financiera
012	Reducir gastos asociados a la nómina así (DF): 3,5% de la nómina 5% horas extras y recargos 20% personal administrativo 2% de la contratación de OPS	Ver informe Costos 2020
013	Reducir en 3% (\$897.695.159) servicios públicos. (DF)	Existe por unidad
014	Cambiar la tercerización imágenes diagnósticas por prestación directa de servicios (ahorro de: \$8.258.689.158). (DF)	No Existe
015	Fortalecer en 5% el ingreso proveniente de stakeholders con beneficio público	No Existe
016	Incrementar al 96% el índice de satisfacción del usuario	Indicador 2020 Satisfacción del usuario 95%
017	Diseñar e implementar una (1) Estrategia de Gestión Territorial en Salud orientada a fortalecer los procesos comunitarios e intersectoriales en la Subred Norte (PTS)	No Existe
018	Diseñar e implementar al 75% la estrategia de cuidado a la ciudadanía. (PDD)	Informe PSPIC
019	Implementar el 100% del programa de organización, integralidad e integración de servicios especializados en cada una de las UMHEs de la Subred Norte.	No Existe
020	Actualizar al 100% el portafolio de servicios institucional de acuerdo a los servicios ofertados. (DF)	Por Actualizar
021	Elaborar e implementar al 70% el plan de comunicaciones para la divulgación de los servicios ofertados, midiendo los resultados obtenidos, frente a la expansión, apertura y adherencia de servicios	No Existe
022	Habilitar servicios ajustados a tipología de portafolios y acreditar 3 unidades de servicios de salud así USS UMHEs Engativá, CAPS Chapinero y Boyacá Real. (DF)	No Existe

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 26 DE 50
		FECHA: 31/01/2024

ID	META	LÍNEA BASE
023	Mejorar en 10% la capacidad académica de acuerdo a la capacidad instalada ofertada, a través de convenios de docencia y servicios.	Capacidad académica 2020 I semestre 48%
024	Implementar el 50% de la arquitectura empresarial desoluciones (PTS).	No Existe
025	Incrementar en 15% el número de colaboradores sensibilizados en la cultura de seguridad del paciente y humanización a través de la capacitación al personal asistencial.	Informe humanización
026	Implementar en un 80% la contratación digital utilizando herramientas tecnológicas que disminuyan la firma física de documentos, contribuyendo a la política de cero papel	No Existe
027	Diseñar e implementar herramientas que garanticen la apropiación de una cultura de autocontrol	No Existe
028	Fortalecer ingreso proveniente del CIS-Norte en \$826.919.695 (DF)	No Existe
029	Certificar a la Subred Norte en buenas prácticas clínicas (UdeA)	Informe Gestión del Conocimiento
030	Implementar el 100% de las estrategias de habilitación y acreditación, necesarias para incluir un hospital universitario en el portafolio de servicios. (PDD)	No Existe
031	Ejecutar el 100% del programa de salud mental integral en la Subred Norte (PDD)	Programa Conscientemente
032	Programa de inducción y reinducción	
033	Cubrir el 100% de las vacantes asignadas y crear el 100% de empleos temporales asignados a la Subred Norte. (PDD)	Informe de Talento Humano
034	Implementar al 95% el intercambio recíproco de la información en la historia clínica (PDD)	No Existe
035	Diseñar, desarrollar e implementar la agenda estratégica digital, que incluya áreas de infraestructura, conectividad, facturación electrónica, digitalización de soportes, historia clínica electrónica. (PDD)	No Existe

Tabla 9: Metas institucionales de la Subred Norte
Fuente: Plan estratégico de tecnologías de la información - PETI

Tendencias tecnológicas

NOMBRE	DESCRIPCIÓN
Uso de nube- Plataforma como servicio	Plataforma de correo en la nube para garantizar confiabilidad y almacenamiento escalable
Automatización de procesos con motor RPA (Robotic Process Automation)	Robotización de procesos administrativos y trámites que tengan actividades repetitivas susceptibles de automatización, mejorando los tiempos de respuesta hacia el cliente final

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 27 DE 50
		FECHA: 31/01/2024

NOMBRE	DESCRIPCIÓN
Software para análisis de datos descriptivo	Aplicativo que permita a partir un conjunto de datos realizar su análisis descriptivo facilitando la identificación de características de la data que permitan ajustar los procesos
Software para análisis de datos predictivo	Aplicativo que permita a partir un conjunto de datos realizar su análisis predictivo facilitando la identificación de tendencias que permitan ajustar los procesos
Software de inteligencia artificial	Aplicativo que permita a partir un conjunto de datos aplicar algoritmos de inteligencia artificial facilitando la identificación de clasificación y regresión de nuevos datos que permitan ajustar los procesos
Blockchain	Control y trazabilidad en las cadenas de abastecimiento y en los trámites de la entidad
Gestión y análisis de datos estructurados (Motores ETL-ELT, Bodegas de datos y datamarts)	Consolidación de las diferentes fuentes de información de la entidad en un único repositorio que facilite la consulta centralizada de información
Plataforma colaborativa	Aplicativo que facilite la comunicación multimedial entre el personal de los procesos permitiendo la trazabilidad, almacenamiento y seguimiento de las comunicaciones
Internet de las cosas (IOT)	Plataforma que permita la gestión e interconectividad entre los dispositivos de monitoreo, sensores y biomédicos con capacidades de conectividad cableada o wifi a la red, facilitando la recolección y centralización de los datos generados
Arquitectura de sistemas orientada a Microservicios	Plataforma que permita la migración y gestión de servicios monolíticos a microservicios en el caso de aplicaciones web como la intranet, aprovechando de manera eficiente y escalable la actual infraestructura de virtualización
Máquinas virtuales (Virtualización de hardware)	Fortalecer la actual infraestructura de virtualización en vmware
Virtualización de sistema operativo en contenedores (Docker)	Plataforma que permita la migración y gestión de servicios monolíticos a microservicios en el caso de aplicaciones web como la intranet, aprovechando de manera eficiente y escalable la actual infraestructura de virtualización
Metodologías ágiles	Mejorar la calidad de los desarrollos propios de la institución
Devops	Automatizar el control, monitoreo, implementación y cambio de la infraestructura informática de la institución

Tabla 10: Tendencias Tecnológicas
Fuente: Plan estratégico de tecnologías de la información - PETI

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 28 DE 50
		FECHA: 31/01/2024

Modelo Operativo de Procesos

A continuación, se describe la estructura del mapa de procesos de la entidad, el cual representa el comportamiento de ésta, dando orientación a cómo se gestiona las actividades para dar cubrimiento a sus objetivos y metas estratégicas.

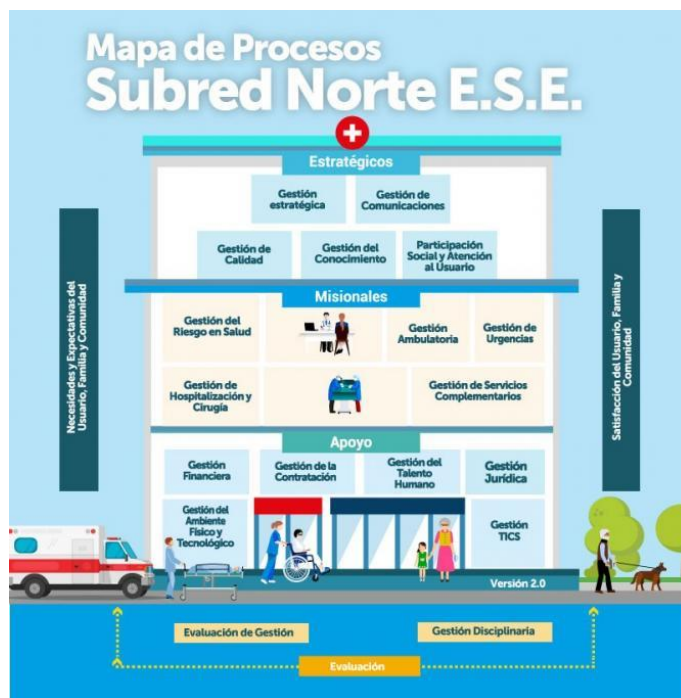


Ilustración 7: Mapa de procesos institucional

Fuente: <https://www.subrednorte.gov.co/transparencia/informacion-entidad/mapa-procesos> Fecha: 19 de diciembre de 2022

Descripción de los procesos

Procesos estratégicos

Nombre de procesos	Objetivo
Gestión estratégica	Se enfoca en las definir las políticas, estrategias y líneas de acción generales para el direccionamiento de la entidad. De acuerdo con la anterior, se definieron en la Subred Integrada de Servicios de Salud Norte ESE, dentro de este grupo cuatro procesos
Participación social y atención al usuario	
Docencia e investigación	
Gestión de calidad	

Tabla 11: Procesos Estratégicos

Fuente: Plan estratégico de tecnologías de la información - PETI

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 29 DE 50
		FECHA: 31/01/2024

Procesos misionales

Nombre de procesos	Objetivo
Gestión del riesgo en salud	El macroproceso misional se centra en generar valor durante el proceso de atención a nuestros usuarios, incidiendo directamente en su satisfacción. Para este efecto se definieron cinco procesos con sus correspondientes procedimientos.
Gestión ambulatoria	
Gestión de urgencias	
Gestión de hospitalización y cirugía	
Gestión de servicios complementarios	

Tabla 12: Procesos Misionales

Fuente: Plan estratégico de tecnologías de la información - PETI

Procesos de apoyo

Nombre de procesos	Objetivo
Gestión financiera	En el macroproceso de apoyo se enmarcan las actividades relacionadas con la entrega a los diferentes procesos de los recursos necesarios en cuanto a personas, maquinaria y materia prima, para poder generar el valor agregado y la satisfacción del usuario. La Subred Norte ESE definió seis procesos.
Gestión de la contratación	
Gestión jurídica	
Gestión TICS	
Gestión del ambiente físico y tecnológico	
Gestión del talento humano	

Tabla 13: Procesos de Apoyo

Fuente: Plan estratégico de tecnologías de la información - PETI

Procesos de evaluación y control

Nombre de procesos	Objetivo
Evaluación de gestión	El grupo de procesos de evaluación permite generar los controles y mejoras al sistema de gestión.
Gestión disciplinaria	

Tabla 14: Procesos de Evaluación y Control Fuente:

Plan estratégico de tecnologías de la información - PETI

Alineación de TI con los procesos

En el siguiente cuadro se presenta la alineación de los recursos de soporte de TI con los procesos más representativos de acuerdo con los objetivos institucionales, las estrategias de TI y el mapa de procesos de la Entidad.

ID	Proceso	Categoría	Sistema de Información
1	Gestión estratégica	Estratégicos	Dinámica Gerencial Hospitalaria
			Correo institucional Outlook 365
			AgilSalud
			Servinte Clinical Suite Enterprise

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 30 DE 50
			FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
2	Participación social y atención al usuario		Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
3	Docencia e investigación		Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 31 DE 50
			FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
4	Gestión de calidad		Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA

Tabla 15: Alineación con los procesos Estratégicos
Fuente: Plan estratégico de tecnologías de la información - PETI

ID	Proceso	Categoría	Sistema de Información
5	Gestión del riesgo en salud	Misional	Mesa de servicios GLPI
			Voz IP
			Moodle

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 32 DE 50
		FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
			Sistema de Gestión Documental ORFEO
			Correo institucional Outlook 365
			Internet/Intranet
			Portal WEB
			ZIMBRA
6	Gestión ambulatoria		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
7	Gestión de urgencias		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 33 DE 50
			FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
8	Gestión de hospitalización y cirugía		Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
			Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA
9	Gestión de servicios complementarios		Servinte Clinical Suite Enterprise
			Correo institucional Outlook 365
			Dinámica Gerencial Hospitalaria
			Sinergys
			Hipocrates
			Servinte Clinical Suite One
			Servinte Clinical Suite
			Mesa de servicios GLPI
			Voz IP

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 34 DE 50
		FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
			Internet/Intranet
			Portal WEB
			Moodle
			Sistema de gestión documental ORFEO
			ZIMBRA

Tabla 16: Alineación con los procesos misionales
Fuente: Plan estratégico de tecnologías de la información - PETI

ID	Proceso	Categoría	Sistema de Información
10	Gestión financiera	Apoyo	Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Portal WEB
			Voz IP
11	Gestión de la contratación		Mesa de servicios GLPI
			Servinte Clinical Suite Enterprise
			Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
12	Gestión jurídica		Portal WEB
			Voz IP
			Mesa de Servicios
			Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
13	Gestión TICS	Correo institucional Outlook 365	
		Portal WEB	
		Mesa de Servicios	
		Servinte Clinical Suite Enterprise	
		Correo electrónico ZIMBRA	
		Sistema de Gestión Documental ORFEO	
		Internet/Intranet	
		Correo institucional Outlook 365	
		Mesa de servicios GLPI	
		Portal WEB	

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 35 DE 50
			FECHA: 31/01/2024

ID	Proceso	Categoría	Sistema de Información
14	Gestión del ambiente físico y tecnológico		Voz IP
			Gestión Dispositivos
			Servinte Clinical Suite Enterprise
			Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Mesa de servicios GLPI
			Voz IP
			Portal WEB
15	Gestión del talento humano		Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Internet/Intranet
			Correo institucional Outlook 365
			Portal WEB
			Voz IP
			Correo electrónico ZIMBRA
			Mesa de servicios GLPI
			Sinergy
			Mesa de Servicios

Tabla 17: Alineación con los procesos de apoyo
Fuente: Plan estratégico de tecnologías de la información - PETI

ID	Proceso	Categoría	Sistema de Información
16	Evaluación de gestión	Evaluación y Control	Sistema de Gestión Documental ORFEO
			Correo electrónico ZIMBRA
			Correo institucional Outlook 365
			Internet/Intranet
			Voz IP
			Portal WEB
			Mesa de servicios GLPI
17	Gestión disciplinaria		Correo electrónico ZIMBRA
			Sistema de Gestión Documental ORFEO
			Correo institucional Outlook 365
			Voz IP
			Mesa de servicios GLPI
			Internet/Intranet
			Portal WEB

Tabla 18: Alineación con los procesos de evaluación y control

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 36 DE 50
		FECHA: 31/01/2024

Fuente: Plan estratégico de tecnologías de la información - PETI

Alineación de MSPI con el Estándar de Gerencia de la Información

A continuación, se presenta los estándares de Gerencia de la Información relacionados con el Modelos de Seguridad y privacidad de la información:

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
Estándares de Gerencia de la Información	Estándar 143. Código: (GI2)	Existe un proceso para planificar la gestión de la información en la organización; este proceso está documentado, implementado y evaluado en un plan de gerencia de la información, e incluye: - La identificación de las necesidades de información. - Un proceso de implementación basado en prioridades. - La recolección sistemática y permanente de la información necesaria y relevante que permita a la dirección y a cada uno de los procesos, la toma oportuna y efectiva de decisiones. - Flujo de la información. - Minería de datos. - Almacenamiento, conservación y depuración de la información. - Seguridad y confidencialidad de la información. - Uso de la información. - El uso de nuevas tecnologías para el manejo de la información. - Recolección sistemática de las necesidades, las opiniones y los niveles de satisfacción de los clientes del sistema de información. - Cualquier disfunción en el sistema de información es recolectada, analizada y resuelta. - La información soporta la gestión de los procesos relacionados con la atención al cliente de la organización. - Identificación de espacios gerenciales y técnicos para el análisis de la información. - Definición de indicadores corporativos que incluyan: Seguridad del paciente, humanización, gestión del riesgo y gestión de la tecnología. - Comparación con mejores prácticas. - Sistema de medición, evaluación y mejoramiento del plan.
	Estándar 146. Código: (GI5)	Existen mecanismos estandarizados, implementados y evaluados para garantizar la seguridad y confidencialidad de la información - La seguridad y la confidencialidad. - Acceso no autorizado. - Pérdida de información. - Manipulación. - Mal uso de los equipos y de la información, para fines distintos a los legalmente contemplados por la organización.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 37 DE 50
		FECHA: 31/01/2024

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
		Deterioro, de todo tipo, de los archivos. Los registros médicos no pueden dejarse o archivarse en sitios físicos donde no esté restringido el acceso a visitantes o personal no autorizado. Existe un procedimiento para la asignación de claves de acceso. Existencia de backups y copias redundantes de información. Control documental y de registros. Indicadores de seguridad de la información.
	Estándar 147. Código: (GI6)	Existe un mecanismo definido implementado, evaluado y formal para transmitir los datos y la información. La transmisión garantiza: Oportunidad. Facilidad de acceso. Confiabilidad y validez de la información. Seguridad. Veracidad. Oportunidad. Facilidad de acceso. Confiabilidad y validez de la información. Seguridad. Veracidad.
	Estándar 148. Código: (GI7)	Existen procesos para la gestión y minería de los datos, que permitan obtener la información en forma oportuna, veraz, clara y conciliada. Esto incluye: La transmisión del dato. La definición de responsables de cada paso en la gestión del dato. Los permisos asignados a cada responsable. La validación y la conciliación entre los datos recolectados y gestionados en forma física y/o electrónica. La generación de información útil en los niveles operativos. La evaluación de la calidad y coherencia de datos generados.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 38 DE 50
		FECHA: 31/01/2024

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
	Estándar 150. Código: (GI9)	La gestión de la información relacionada con los registros clínicos, sea en medio físico o electrónico, garantiza la calidad, la seguridad y la accesibilidad de los mismos. Incluye: Orden. Legibilidad y concordancia clínico-patológica. Claridad y actualización de los registros clínicos. Adecuado archivo de los registros clínicos y fácil disponibilidad cuando sean requeridos. Auditoría sistemática y periódica a la calidad de forma y contenido de los registros clínicos. Garantía de la custodia de los registros clínicos. Unicidad de los registros clínicos para cada usuario. Sistema de identificación y numeración unificado para todos los registros clínicos. Esquema del proceso de transición a historia clínica electrónica. Sistemas de chequeo para evitar errores en la identificación de los usuarios. Sistemas de alarma redundante para las condiciones que lo ameriten. Procesos para la entrega de los resúmenes de historia clínica solicitados por las autoridades competentes o los mismos usuarios. La organización garantiza que en los procesos de la gerencia de información es posible verificar si el usuario ha asistido previamente a la institución, en qué fechas, qué profesional lo ha atendido, qué exámenes se le han ordenado, etc. Cuando se tenga un sistema mixto de registro de atenciones (electrónico y manual), se debe garantizar que haya un solo sistema de identificación del paciente, para que el contenido de las atenciones esté disponible para cualquier prestador y se le pueda hacer auditoría integral al registro.
	Estándar 155. Código: (GIMCC1)	La gestión de las oportunidades de mejora consideradas en el proceso organizacional de mejoramiento continuo, que apliquen al grupo de estándares, se desarrolla teniendo en cuenta: El enfoque organizacional del mejoramiento continuo. La implementación de oportunidades de mejora priorizadas y la remoción de barreras de mejoramiento, por parte de los equipos de autoevaluación, los equipos de mejora y los demás colaboradores de la organización." La articulación de oportunidades de mejora que tengan relación entre los diferentes procesos y grupos de estándares. El seguimiento a los resultados del mejoramiento, la verificación del cierre de ciclo, el mantenimiento y el aseguramiento de la calidad. La comunicación de los resultados.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 39 DE 50
			FECHA: 31/01/2024

GRUPO DE ESTANDARES	ESTANDAR	ESTÁNDAR / CRITERIO AFECTADO
	Estándar 151. Código: (GI10)	Existe un plan de contingencia diseñado, implementado y evaluado que garantice el normal funcionamiento de los sistemas de información de la organización, sean manuales, automatizados, o ambos. Cualquier disfunción en el sistema es recolectada, analizada y resuelta. Lo anterior incluye mecanismos para prevenir eventos adversos relacionados con el manejo de los sistemas de información en especial alarmas en historia clínica.

Tabla 19: Estándar de Gerencia de la Información

Estructura orgánica

La Subred Integrada de Servicios de Salud Norte E.S.E, para el cumplimiento de su misión establece la siguiente estructura orgánica:

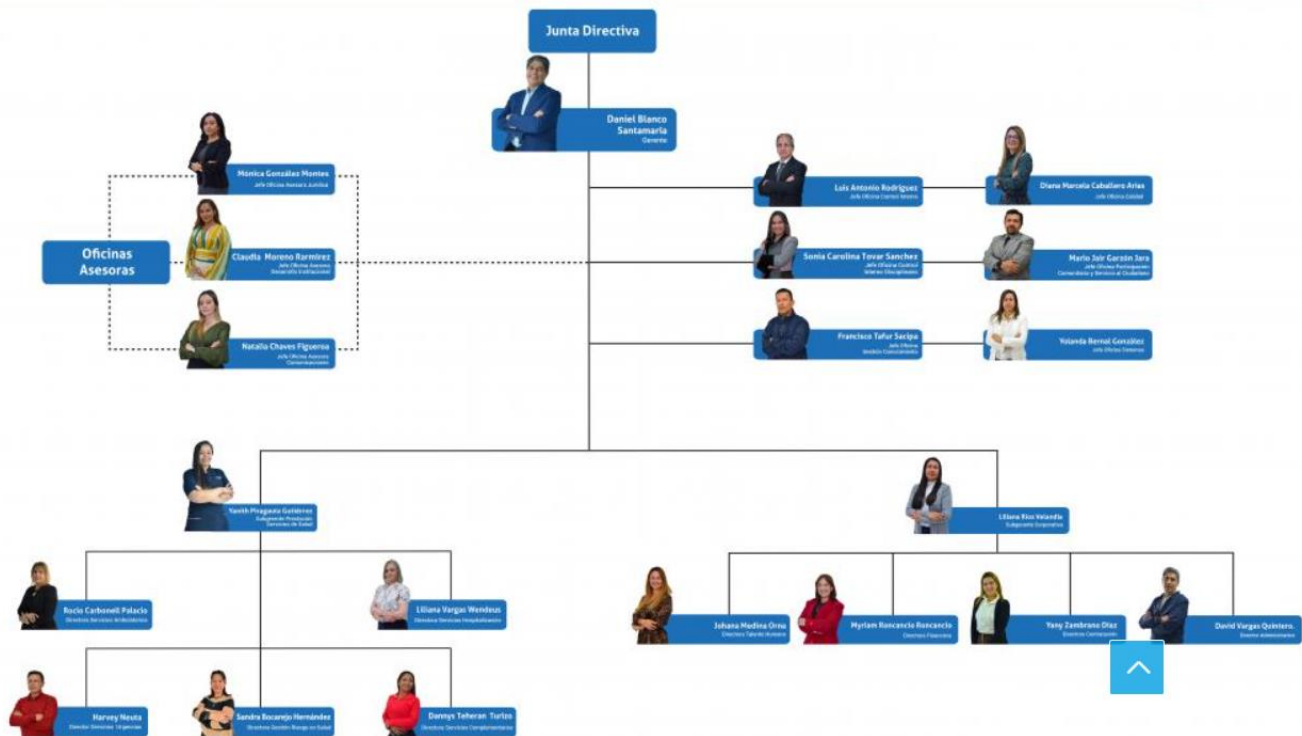


Ilustración 8: Estructura orgánica institucional

Fuente: <https://www.subrednorte.gov.co/node/18>, Fecha: 30 de junio de 2023

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 40 DE 50
		FECHA: 31/01/2024

8.4.2.2 Liderazgo

La alta dirección en compañía del grupo de seguridad de la información participa activamente demostrado liderazgo y compromiso con respecto al MPSI, estableciendo las políticas, objetivos, recursos; realizando socializaciones sobre la importancia y logros del MPSI, promoviendo la mejora continua y se ha asignado los respectivos roles y responsabilidades.

8.4.2.3 Políticas

Política de Seguridad y Privacidad de la Información:

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

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

Objetivos:

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

Adicionalmente la Subred Integrada de Servicios de Salud Norte E.S.E, cuenta con el manual de políticas de seguridad y privacidad de la información, en su versión 2 con el código AP-GI-M-02-02 y aprobado el 21 de octubre de 2021

8.4.2.4 Procedimientos de Seguridad de la Información.

En cumplimiento a la norma ISO 27001 y las necesidades de la Subred Integrada de Servicios de Salud Norte E.S.E, durante esta etapa se pretende identificar y documentar los procedimientos que garanticen un apropiado funcionamiento del MSPI.

En este sentido se revisará la documentación con la cual se cuenta y se alineará con los requisitos del MSPI, utilizando la Guía No 3. Procedimientos de Seguridad de la Información de MinTIC.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 41 DE 50
		FECHA: 31/01/2024

8.4.2.5 Roles y Responsabilidades de Seguridad y Privacidad de la Información

Este es una de las primeras actividades para implementar el MSPI, en él se definirá la estructura organizacional con funciones y responsabilidades, esto con el fin, que cada una de las tareas a realizar se designe el personal con habilidades y actitudes necesarias para desempeñar las funciones con eficiencia y se genere un producto de calidad.

Este documento se puede realizar referenciando la Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información, el cual nos ayudara a la elaboración de dicho documento.

8.4.2.6 Inventarios de Activos de información (AI)

Un Activo de Información - AI, según la ley 1712 de 2014, es todo aquel elemento de información que sea producido o recibido por la Subred Integrada de Servicios de Salud Norte E.S.E en el ejercicio de sus funciones. Incluye la información en forma impresa o electrónica, software, hardware, recurso humano, archivos, bases de datos, videos e imágenes.

Para la clasificación de AI la Subred Integrada de Servicios de Salud Norte E.S.E utilizará el proceso y la tipología definidos en la Guía para la Gestión y Clasificación de Activos de Información de MinTIC. En este sentido, es preciso definir que los responsables de los procesos que se encuentran dentro del alcance del SGSI-MSPI, son los encargados de suministrar la información, valoración, ubicación y clasificación de los mismos.

8.4.2.7 Integración del MSPI con el Sistema de Gestión documental.

En esta sección es importante establecer y alinear el Sistema el Gestión Documental con el MSPI, para tal fin la Guía 6 – Gestión Documental, nos permite establecer esta relación.

8.4.2.8 Plan de seguridad y privacidad de la información.

El plan de seguridad y privacidad de la información se encuentra dentro de los lineamientos del Modelo Integrado de Planeación y Gestión, alineado con la Políticas de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información, en la Dimensión Gestión con Valores para Resultados

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 42 DE 50
		FECHA: 31/01/2024

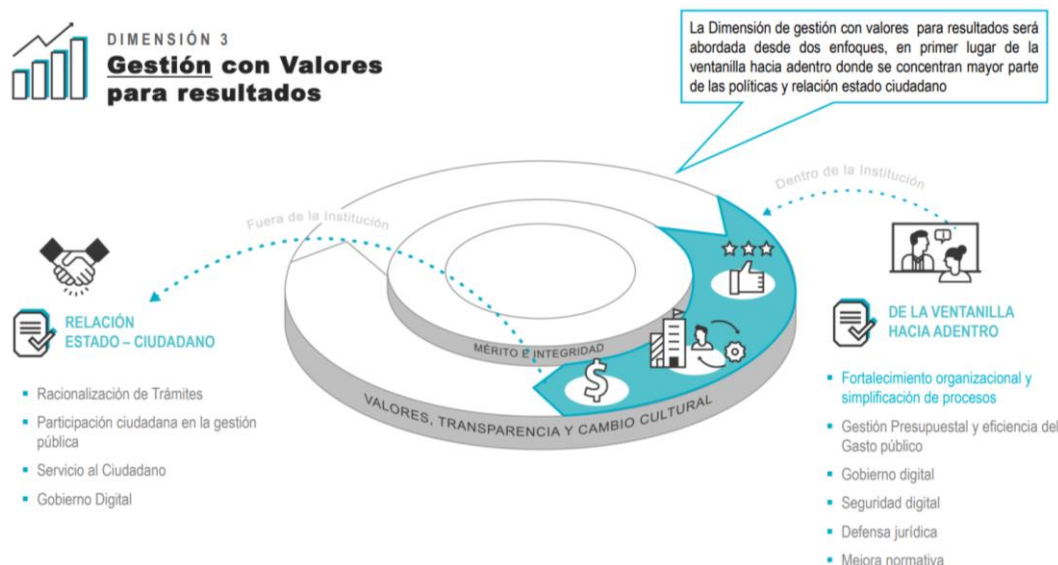


Ilustración 9: Dimensión 3 MIPG, Fuente: Modulo 3 Gestión con valores para resultados

El plan de seguridad y privacidad de la información se encuentra dentro de las acciones planteadas en la implementación del Sistema de seguridad y privacidad de la información - SGSI, dando cumplimiento de los requisitos en la implementación de la política de Gobierno Digital.

8.4.2.9 Identificación, Valoración Y Tratamiento de Riesgos.

Con el fin de mantener una adecuada organización para la Gestión de los Riesgos de Seguridad de la Información (actualizados y controlados) en la Subred Integrada de Servicios de Salud Norte E.S.E; dichos riesgos se adoptarán a través de la Política de Gestión del Riesgo, liderada por oficina de Desarrollo Institucional, que a su vez se ajustan al Modelo de Riesgos definidos por el Departamento Administrativo de la Función Pública – DAFP.

En este sentido, la metodología adoptada por la Subred Integrada de Servicios de Salud Norte E.S.E para el tratamiento de los riesgos de seguridad y privacidad de la información es la definida por MINTIC y debe ser presentada en el documento Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Sistema Integrado de Gestión, actualizado a corte 30 de noviembre de 2023.

De acuerdo con MODELO DE GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL de MINTIC, la identificación y valoración del riesgo de los activos debe ser realizada por la Primera Línea de Defensa – Líderes de Proceso, en cada proceso donde aplique la gestión del riesgo de seguridad de la información, siendo debidamente orientados por el responsable de seguridad de la información de la entidad. El proceso de gestión del riesgo en cuanto a su valoración y tratamiento es sistemático e iterativo, lo cual presume un proceso de mejora continua como se esboza en el plan, con el objetivo de descubrir y planificar el tratamiento oportuno y mantener los riesgos bajo control. En consecuencia, con lo anterior, la metodología y el proceso para la valoración de riesgo lo ilustra el siguiente gráfico.

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 43 DE 50
		FECHA: 31/01/2024

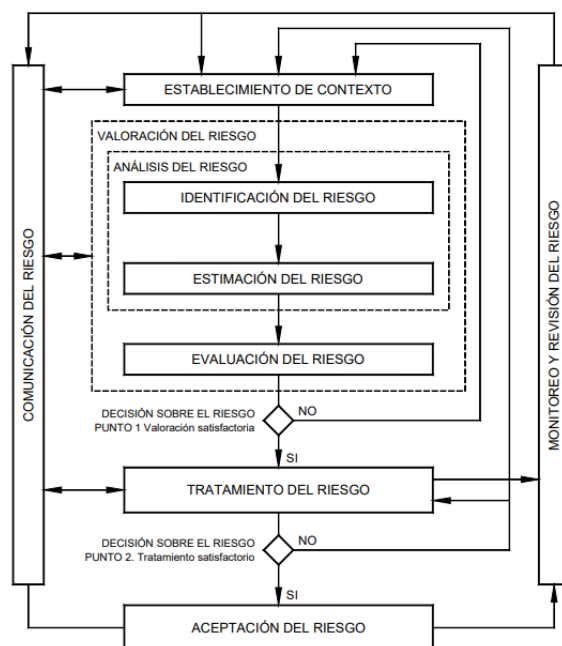


Ilustración 10: Proceso de gestión del riesgo en la seguridad de la información, Fuente: Norma Técnica Colombiana NTC-ISO/IEC 27005

Política de Gestión de Administración de Riesgos de la Subred Integrada de Servicios de Salud Norte E.S.E

Enunciado:

La Subred Integrada de Servicios de Salud Norte E.S.E, se compromete a adoptar los mecanismos y acciones necesarias para una eficaz administración de sus riesgos, de tal forma que se prevengan o minimicen sus impactos, mediante una adecuada identificación, análisis, valoración, priorización y control, orientados a garantizar la integridad, seguridad y la calidad en el desarrollo de sus actividades y la prestación de sus servicios.

Objetivo de la política de gestión de administración de riesgos:

Promover la implementación de metodologías que permitan la articulación del sistema de gestión de riesgo institucional con el fin de alcanzar niveles aceptables de riesgos residuales para poder cumplir los objetivos misionales, estratégicos y de procesos con participación activa de los colaboradores y de acuerdo a los niveles de responsabilidad establecida en las líneas de defensa acorde con la Política de Atención Integral en Salud y su modelo de atención

- Establecer estrategias eficaces de control para los riesgos de mayor impacto para la entidad
- Promover el seguimiento oportuno a las acciones establecidas para la mitigación de los riesgos identificados
- Promover mecanismos orientados a fomentar el conocimiento en la gestión del riesgo en todos los colaboradores de la entidad
- Reforzar la autorregulación de los procesos institucionales, con participación activa de los colaboradores y de acuerdo a la responsabilidad establecida en las líneas de defensa

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 44 DE 50
		FECHA: 31/01/2024

Alcance de la política de gestión de administración de riesgos:

La política de gestión de administración de riesgos debe ser extensible y aplicable a todos los procesos de la entidad. En el caso de los riesgos de **seguridad digital, SARLAFT y riesgos de corrupción estos se deben gestionar de acuerdo con los criterios diferenciales descritos en el modelo de seguridad y privacidad de la información**

La Subred Integrada de Servicios de Salud Norte E.S.E, dentro del alcance de la POLÍTICA DE GESTIÓN Y ADMINISTRACIÓN DEL RIESGO, aprobada en el comité institucional de gestión y desempeño el día 22 de octubre de 2022, incluyó el compromiso en la gestión de los riesgos de seguridad digital definidos en el Modelos de Seguridad y privacidad de la información.

8.4.2.10 Sensibilización y concienciación

La oficina de Sistemas de Información – TICS con el apoyo de la oficina de comunicaciones, son los encargados de elaborar y desplegar el Plan de Sensibilización de Seguridad de la Información, cuyos objetivos consisten en: generar una cultura de seguridad de información, el establecimiento de compromisos en servidores y colaboradores en aspectos relacionados con el MSPI, el tratamiento adecuado de la información y el control de riesgos de Seguridad de Información.

8.4.2.11 Comunicación

La oficina de Sistemas de Información – TICS con el apoyo de la oficina de comunicaciones, a través del plan de comunicaciones de la entidad, se encargarán de comunicar a todos los funcionarios, contratistas y partes interesadas sobre la implementación del MSPI-SGSI, con énfasis en los roles y responsabilidades que cada uno desempeña, los posibles riesgos y las consecuencias del incumplimiento de las políticas de Seguridad de Información.

8.4.3 Implementación

En esta fase se lleva a cabo el establecimiento de los controles de seguridad, el cumplimiento del plan de sensibilización y/o concientización, la ejecución de actividades por dominio, actividades de mitigación de los riesgos de seguridad y privacidad de la información y seguimiento a los indicadores de gestión

8.4.4 Evaluación de desempeño

El seguimiento continuo al sistema, la evaluación de indicadores, la ejecución de auditorías y planes de mejora, permitirán determinar la fortaleza del sistema desarrollado y la eficacia de los controles implementados.

En este sentido, se deben ejecutar las siguientes acciones:

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 45 DE 50
		FECHA: 31/01/2024

- Verificar la implementación de procedimientos y demás controles de supervisión para determinar cualquier violación, procesamiento incorrecto de datos y determinar si las actividades de seguridad se desarrollan de acuerdo con lo previsto.
- Verificar el estado de los activos de información, actualizando periódicamente la matriz correspondiente.
- Verificar el estado del plan de seguridad y el de tratamiento de riesgos.
- Verificar las actividades e incidentes que puedan afectar la eficacia del MSPI.

8.4.5 Mejora continua

En esta fase se realizará mantenimiento y mejora al SGSI de todas aquellas acciones que presenten debilidades o hallazgos negativos o no esperados. Para esta fase la Subred Integrada de Servicios de Salud Norte E.S.E debe:

- Implementar y documentar en el MSPI las mejoras identificadas.
- Tomar medidas correctivas y preventivas y aplicar mejores prácticas sobre incidentes de seguridad.
- Comunicar las mejoras a todos los grupos de interés.
- Alinear las mejoras con los objetivos previstos y necesidades de la Subred

9 PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

El Plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma y se le hace seguimiento trimestralmente.

ACTIVIDAD	ACCIÓN	RESPONSABLE	EVIDENCIA	FECHA INICIO	FECHA FINAL
Realizar el autodiagnóstico del MSPI para identificar las brechas.	Matriz del autodiagnóstico diligenciado	Grupo de Seguridad de la información	Herramienta diagnostica MSPI	1/01/2024	28/02/2024
Seguimiento a Política general de la Seguridad de la Información.	Informes indicadores Política de Seguridad y Privacidad de la Información	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024
Seguimiento al Manual de Políticas de Seguridad y Privacidad de la Información	Informe Seguimiento Manual de Políticas de Seguridad y Privacidad de la Información	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024
	Seguimiento a la política de Control de acceso	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 46 DE 50
		FECHA: 31/01/2024

	Seguimiento a la política de copias de seguridad	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024
	Seguimiento a la Política de Seguridad Física y del entorno	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024
	Seguimiento a la Política de Seguridad de Gestión de Incidentes	Grupo de Seguridad de la información	Informe Seguimiento	1/01/2024	31/12/2024
Elaboración y/o actualización de instructivos de Seguridad y privacidad de la información	Actualización y/o elaboración de documentos	Grupo de Seguridad de la información	Documentación normalizada	1/04/2024	31/07/2024
Revisión y actualización del inventario de Activos de información	Realizar seguimiento, revisión y actualización del Inventario de Activos de Información.	Grupo de Seguridad de la información	Matriz de Inventario de activos de Información actualizado	31/04/2024	31/09/2024
Análisis de vulnerabilidades	Realizar análisis de vulnerabilidades de los servicios en la nube	Grupo de Seguridad de la información	Informe análisis de vulnerabilidades	1/04/2024	31/04/2024
	Realizar análisis de vulnerabilidades para servicios expuestos a internet	Grupo de Seguridad de la información	Informe análisis de vulnerabilidades	1/08/2024	31/08/2024
	Realizar análisis de vulnerabilidades de la infraestructura on premise	Grupo de Seguridad de la información	Informe análisis de vulnerabilidades	1/12/2024	31/12/2024
Seguimiento al tratamiento de riesgos de Seguridad digital	Realizar seguimiento, revisión y actualización a los riesgos de seguridad	Grupo de Seguridad de la información	Informe del tratamiento de riesgos de seguridad	1/07/2024	31/12/2024
Elaborar el Plan de sensibilización de TICS	Documento con el plan de comunicación, sensibilización y capacitación para la entidad	Grupo de Seguridad de la información	Cronograma de sensibilización	1/01/2024	29/02/2024
Ejecutar el Plan de sensibilización de TICS - de Seguridad de la información			Soporte de ejecución de plan, actas de sensibilización - Piezas comunicativas	1/03/2024	31/12/2024
Informe de la ejecución del Plan de Comunicaciones de TICS			Informe de la ejecución	1/06/2024	31/12/2024

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		CÓDIGO: AP-GI-PL-02
			VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS		PÁGINA: 47 DE 50
			FECHA: 31/01/2024

Plan de recuperación de desastres	Elaborar el Plan de recuperación de desastres	Grupo de Seguridad de la información – oficina de desarrollo institucional	Plan de recuperación de desastres	1/03/2024	30/06/2024
	Aprobación y socialización del plan de recuperación de desastres		Acta de aprobación comité	1/07/2024	31/07/2024
	Seguimiento Plan de recuperación de desastres		Actas de simulacro y socialización	1/08/2024	31/12/2024
Seguimiento de indicadores del SGSI	Informe indicadores	Grupo de Seguridad de la información	Informe de seguimiento	1/09/2024	31/12/2024

Tabla 20: Cronograma de trabajo del MSPI

10 SEGUIMIENTO Y MEDICIÓN

NOMBRE DEL INDICADOR	FORMULA DEL INDICADOR	META	FRECUENCIA
Porcentaje de cumplimiento del Plan de Seguridad y Privacidad de la Información.	$(\text{Número de actividades ejecutadas} / \text{Total de actividades programadas}) \times 100$	80%	Trimestral

Tabla 21: Indicador del plan de seguridad y privacidad de la información

11 BIBLIOGRAFÍA

COMUNICACIONES, M. D. (03 de 08 de 2018). funcionpublica.gov.co. Obtenido de https://www.funcionpublica.gov.co/web/eva/biblioteca-virtual/-/document_library/bGsp2ljUBdeu/view_file/34316352?_com_liferay_document_library_web_portlet_DLPortlet_INSTANCE_bGsp2ljUBdeu_redirect=https%3A%2F%2Fwww.funcionpublica.gov.co%2Fweb%2Feva%2Fbiblio

Gaviria Muñoz, S. (11 de 04 de 2016). Documento CONPES 385. Obtenido de <https://colaboracion.dnp.gov.co/:https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>

ICONTEC. (2013). Compendio seguridad de la información/ICONTEC. Obtenido de https://catalogo.unimilitar.edu.co/:https://catalogo.unimilitar.edu.co/cgi-bin/koha/opacdetail.pl?biblionumber=28324&shelfbrowse_itemnumber=58085

Mintic. (16 de 03 de 2016). Guía para la Gestión y Clasificación de Activos de Información. Obtenido de https://www.mintic.gov.co/:https://www.mintic.gov.co/gestionti/615/articles5482_G5_Gestion_Clasificacion.pdf

Mintic. (s.f.). Sistemas de Gestión de la Seguridad de la Información (SGSI). Obtenido de <https://www.mintic.gov.co/:https://www.mintic.gov.co/gestionti/615/w3-article5482.html?noredirect=1>

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 48 DE 50
		FECHA: 31/01/2024

12 ANEXOS

- Plan de tratamiento de riesgos de seguridad y privacidad de la información
- Autodiagnóstico del MSPI- instrumento MINTIC

CONTROL DEL DOCUMENTO		
Versión	Fecha	Descripción de la modificación
1	19/10/2017	Creación
2	07/02/2019	Se actualiza contenido en general en cumplimiento del acuerdo 642 de 2018
3	27/08/2021	Actualización general y aplicación nueva plantilla institucional.
4	13/10/2023	Actualización al documento y al plan de trabajo
5	31/01/2024	Actualización al documento y al plan de trabajo

Elaborado por:	Revisado por:	Aval Oficina de Calidad:	Aprobó:
Nombre: Jaime Alberto Arévalo Sierra	Nombre: Jairo Fernando Hurtado Valenzuela	Nombre: Diana Marcela Caballero	Nombre: Daniel Blanco
Cargo: Apoyo Profesional Especializado	Cargo: Jefe Oficina de Sistemas	Cargo: Jefe Oficina de Calidad	Cargo: Gerente

	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	CÓDIGO: AP-GI-PL-02
		VERSIÓN: 5
	SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E. GESTIÓN DE LA INFORMACIÓN Y TICS	PÁGINA: 49 DE 50
		FECHA: 31/01/2024

		PLAN DE TRABAJO PLAN ESTRATEGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN																											
		SUBRED INTEGRADA DE SERVICIOS DE SALUD NORTE E.S.E.																											
PLAN ESTRATEGICO / INSTITUCIONAL		Plan de Seguridad y Privacidad de la Información																											
VIGENCIA: 2024																													
Objetivo General:		Definir las actividades del Plan la Seguridad y Privacidad de la Información de la Subred Integrada de Servicios de Salud Norte ESE, por medio de los lineamientos establecidos el ciclo PHVA definido en la norma ISO 27001, el modelo de referencia definido por el Ministerio de Tecnologías de Información, la Política de Gobierno Digital y plataforma estratégica de la Subred Integrada de Servicios de Salud Norte E.S.E., de acuerdo con el modelo del Sistema de Gestión de Seguridad de la Información, con el fin de consolidar la operación y contribuir al logro de los objetivos y requisitos normativos en materia de la Modelo de Seguridad y Privacidad de la Información - MSPI y el Modelo Integrado de Planeación y Gestión (MIPG).																											
Alineos:		Teniendo en cuenta la estructura el mapa de procesos de la Subred Integrada de Servicios de Salud Norte ESE, el plan de seguridad y privacidad de la Información aplica para todos los procesos por su nivel de sensibilidad ya que su daño o pérdida, pueden llevar un impacto negativo de índole legal, reputacional, de imagen y académico para la entidad.																											
No.	Objetivos Específicos	Actividades	Meta / Producto	Responsable	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Primer Seguimiento				Segundo Seguimiento				Tercer Seguimiento				
																	Fecha	Estado	Observación	% Avance Acumulado	Fecha	Estado	Observación	% Avance Acumulado	Fecha	Estado	Observación	% Avance Acumulado	
1	Identificar brechas de Seguridad	Realizar el autodiagnóstico del MSPI	Autodiagnostico MSPI	Oficial de Seguridad de la Información																									
2	Verificar el avance de los indicadores de la política	Seguimiento a Política general de la Seguridad de la Información.	Informe Indicadores Política de Seguridad y Privacidad de la Información	Oficial de Seguridad de la Información																									
3	Seguimiento a la política de Control de acceso	Seguimiento al Manual de Políticas de Seguridad y Privacidad de la Información	Informe Seguimiento	Oficial de Seguridad de la Información																									
4	Seguimiento a la política de copias de seguridad			Oficial de Seguridad de la Información																									
5	Seguimiento a la Política de Seguridad Física y del entorno			Oficial de Seguridad de la Información																									
6	Seguimiento a la Política de Seguridad de Gestión de Incidentes			Oficial de Seguridad de la Información																									
7	Garantizar la actualización, y/o elaboración de instructivos de Seguridad y Privacidad de la Información	Elaboración y/o actualización de Instructivos de Seguridad y privacidad de la Información	Documentación normalizada	Oficial de Seguridad de la Información																									
8	Verificar el estado de los activos de información	Revisión y actualización del Inventario de Activos de Información	Matriz de Inventario de activos de Información actualizado	Oficial de Seguridad de la Información																									
9	Realizar análisis de vulnerabilidades de los servicios en la nube	Análisis de vulnerabilidades	Informe análisis de vulnerabilidades	Oficial de Seguridad de la Información																									
10	Realizar análisis de vulnerabilidades para servicios expuestos a Internet			Oficial de Seguridad de la Información																									
11	Realizar análisis de vulnerabilidades de la infraestructura on premise			Oficial de Seguridad de la Información																									
12	Verificar el tratamiento de los riesgos de seguridad identificados	Seguimiento al tratamiento de riesgos de Seguridad digital	Informe del tratamiento de riesgos de seguridad	Oficial de Seguridad de la Información																									
13	Concientiar y educar a los colaboradores sobre la	Elaborar el Plan de sensibilización de TICs	Documento con el plan de comunicación	Oficial de Seguridad de la Información																									

La última versión de cada documento será la única válida para su utilización y estará disponible en el Listado Maestro de Documentos
No haga copias de este documento porque corre el riesgo de tener una versión desactualizada