PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

SALUD SOGAMOSO ESE 2024

INTRODUCCIÓN

La seguridad de la información, según ISO/IEC 27001:2013, consiste en preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de un proceso de Gestión de Riesgo, (ISO/ IEC 27001 VERSION 2013, 2013), para lo cual, el proyecto busca dar respuesta a las exigencias que el Ministerio de Tecnologías de la Información y las comunicaciones de Colombia, (MinTic), presenta para todas entidades públicas.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse a los siguientes componentes:

TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece la Entidad, observando en todo momento las normas sobre protección de datos personales, así como otros derechos garantizados por la Ley que exceptúa el acceso público a determinada información.

TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

Este documento indica, definiendo plazos anuales, cuáles serán las labores que realizará Salud Sogamoso con el objetivo de lograr el 100% de la implementación del MSPI al interior de todos los procesos de la entidad.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización. Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Las actividades para la administración y la seguridad informática pueden clasificarse en varias categorías como son: seguridad funcional, coordinación, documentación, certificación, acreditación, administración de configuraciones de sistemas y de seguridad informática y manejo de riesgos.

Este documento se elabora con el objetivo de orientar a la Entidad para dar cumplimiento con lo solicitado en el Decreto 612 de 2018 y todas las consideraciones expuestas, dentro de las cuáles se encuentra el decreto 1078 de 2015 y los instrumentos para implementar la Estrategia de Gobierno Digital, dentro de los cuales se exige la elaboración por parte de cada entidad, de un Plan de Seguridad y Privacidad de la Información.

En el presente documento adoptó la concepción, metodología, lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones –MinTIC-, que conforman la Estrategia de Gobierno Digital, la cual está soportada en los LINEAMIENTOS PARA LA ELABORACIÓN DEL PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION y el MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. OBJETIVO

Fortalecer, liderar y establecer las estrategias para la gestión, integralidad, confidencialidad, seguridad y privacidad de la Información en Salud Sogamoso E.S.E. que permitan minimizar los riesgos de pérdida de activos de la información y estén alineadas a la estrategia y modelo integrado de gestión y acordes con las necesidades de la Entidad y los lineamientos de la estrategia de Gobierno Digital.

1.1. Objetivos específicos

El PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION de Salud Sogamoso E.S.E.- cuenta con los siguientes objetivos específicos acordes con las necesidades de la Entidad y las dimensiones de Gobierno Digital:

- Definir las responsabilidades relacionadas con el manejo de la seguridad, durante el transcurso del año en Salud Sogamoso ESE. Establecer una metodología de gestión de la seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información. Garantizar que los usuarios tienen acceso a la información a través medidas de seguridad con la garantía de calidad y confidencialidad. Implementar las auditorías externas para identificar las debilidades del sistema y las áreas a mejorar.
- Garantizar la continuidad de las operaciones necesarias de la empresa tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.
- Mantener el plan para la transición de IPv4 a IPv6 .

2. ALCANCE DEL PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

El Plan Estratégico de Seguridad de la Información busca la implementación del Sistema de Gestión de Seguridad y privacidad de la Información y la estrategia de seguridad digital y tendrá en cuenta todos los procesos que se ejecutan en Salud Sogamoso E.S.E. donde la finalidad es el diagnóstico, análisis, definición y planeación del manejo de la seguridad de la información y será actualizado cada dos años.

3. MARCO NORMATIVO PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION

Ley 527 de 1999: Define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, así mismo introduce el concepto de equivalente funcional, firma electrónica como mecanismos de autenticidad, disponibilidad y confidencialidad de la información. (CONGRESO NACIONAL, 1999).

CONPES 3670 de 2010. "Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones".

CONPES 3701 de 2011. "Lineamientos de Política para Ciberseguridad y Ciberdefensa" Ley 872 de 2003. "Por la cual se crea el sistema de gestión de la calidad en la Rama Ejecutiva del Poder Público y en otras entidades prestadoras de servicios".

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 del Espectro y se dictan otras disposiciones".

Ley 39 de 1981. Sobre microfilmación y certificación de archivos.

Ley 594 de 2000. "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones".

Ley 1712 de 2024: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. (CONGRESO DE LA, 2024)

Decreto 103 de 2015: Por la cual se reglamenta parcialmente la ley 1712 de 2024 y se dictan otras disposiciones, en cuanto a la publicación y divulgación de la información. (PRESIDENCIA DE LA, 2015)

Decreto 2609 de 2012: Por el cual se dictan disposiciones en materia de gestión documental y gestión documental electrónica. (2012)

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones. (MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS, 2012)

Ley 1273 de 2009: Ley la cual se crea y se protege el bien jurídico de la información y los datos personales.

Ley 1581 de 2012: Ley Estatutaria por la cual se reglamenta el artículo

15 de la Constitución política, relativo a la intimidad personal y el Habeas Data, a través de esta norma se dictan disposiciones generales para la protección de datos personales.

Ley 594 de 2000: Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. (CONGRESO D. L., 2000)

Decreto 612 de 2018, "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado", donde se encuentra el presente PLAN DE PRIVACIDAD Y SEGURIDAD DE LA INFORMACION como uno de los requisitos a desarrollar para cumplir con esta normativa.

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".

Manual de Gobierno Digital – MINTIC.

Modelo de Seguridad y Privacidad de la Información – MINTIC.

4. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Salud Sogamoso E.S.E. se compromete a un eficiente manejo de la información, utilizando recursos adecuados, apoyados en lineamientos que garanticen la confidencialidad, privacidad, seguridad y confiabilidad de la información.

Salud Sogamoso E.S.E. entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de nuestra entidad.

Salud Sogamoso E.S.E., Tiene riesgos identificados, con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés.

El contenido de esta política aplica a la entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza de sus usuarios, entes de control y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.

- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de Salud Sogamoso E.S.E.
- Garantizar la continuidad de Salud Sogamoso E.S.E. Frente a incidentes.
- Salud Sogamoso E.S.E. Ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades y a los requerimientos regulatorios.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de Salud Sogamoso E.S.E.:

• Salud Sogamoso E.S.E. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades empresariales , y a los requerimientos regulatorios que le aplican a su naturaleza.

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

• Salud Sogamoso E.S.E. protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.

• Salud Sogamoso E.S.E. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

• Salud Sogamoso E.S.E. protegerá su información de las amenazas originadas por parte del personal.

• Salud Sogamoso E.S.E. protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

• Salud Sogamoso E.S.E. controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

• Salud Sogamoso E.S.E. Implementará control de acceso a la información, sistemas y recursos de red.

• Salud Sogamoso E.S.E. garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

• Salud Sogamoso E.S.E. garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

• Salud Sogamoso E.S.E. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

• Salud Sogamoso E.S.E. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas y adoptadas en el MANUAL DE GERENCIA Y SEGURIDAD DE LA INFORMACIÓN.

5. ANÁLISIS DEL ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.1 Análisis de brecha MSIP

Apoyados en la herramienta "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A" se obtuvieron los siguientes resultados de análisis de brecha sobre la efectividad de los controles, obteniendo los siguientes resultados:

Documento que hace parte de este Plan

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	50	100	EFECTIVO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	44	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	71	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	65	100	GESTIONADO
A.9	CONTROL DE ACCESO	68	100	GESTIONADO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	47	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	49	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	44	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	56	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	80	100	GESTIONADO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	40	100	REPETIBLE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	60	100	EFECTIVO
A.18	CUMPLIMIENTO	68,5	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		**54**	**100**	EFECTIVO

En la tabla y grafico anterior Se evidencia que se debe trabar en los siguientes temas:

- Políticas de Seguridad de la Información
- Organización de la seguridad de la información.
- Instrumento de identificación de la línea base de seguridad administrativa y técnica hoja levantamiento de información
- Relaciones con los proveedores
- Aspectos de seguridad de la información de la gestión para la continuidad del negocio

La calificación total es de 54 de 100 la cual es susceptible de evaluación continua.

Gracias a este análisis se priorizan los seis temas anteriores.

En cuanto al análisis de brecha para el avance se diligenciará la matriz PHVA del instrumento de evaluación del MSPI. Con esta herramienta se determinar las acciones a seguir en cada fase del modelo.

En cuanto a la madurez del MSPI se tiene el siguiente análisis:

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

		NIVEL DE CUMPLIMIENTO
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Inicial	SUFICIENTE
	Repetible	SUFICIENTE
	Definido	INTERMEDIO
	Administrado	INTERMEDIO
	Optimizado	CRÍTICO

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 cuenten 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.

TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO

CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

De acuerdo al análisis de brecha se priorizan para el año 2024 las actividades faltantes para alcanzar el nivel 3.

- Análisis de brecha Transición de IPv4 a IPv6 se debe gestionar para lograr la transición a 31 de Diciembre del año 2025
- Gestión de Información atendiendo al resultado establecido en la hoja de Madurez del instrumento de evaluación MSPI, en el campo cumplimiento nivel gestionado donde el estado evaluado del ítem esta en grado menor.

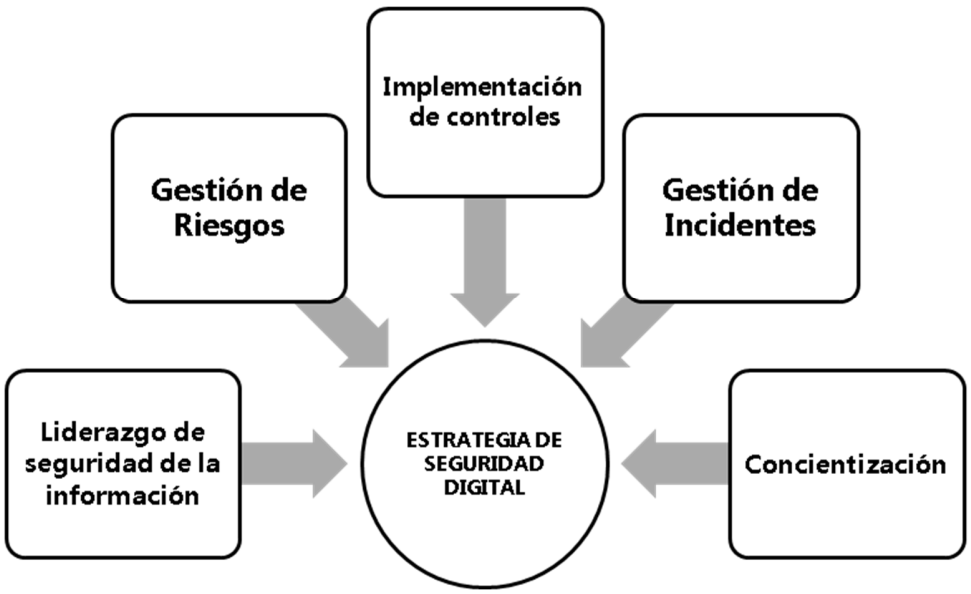
CONTROL DE	USUARIOS			
	Ciudadanía-EAPB-Gobierno Nacional	Entidades Publicas Privadas – Persona Natural –Comunidades Etnicas – Asociaciones de Usuarios – Comunidad en general – Entes territoriales – Rama judicial - Entes de Control – Cooperación Internacional – Gremios.		
PRESENTACIÓN	ACCESO A LA INFORMACIÓN			
	Consulta en Linea tramites en CITAS WEB y PQRDS– PAGINA WEB – Boletines y Comunicados – Reportes – Estadísticas – Datos Abiertos			
	Directorio Activo – CNT – Servidores, hardware y software			
CONTINUIDAD DEL NEGOCIO	CALIDAD DE DATOS			
	Parametros databases	Modulo de Metadatos MODULOS ASISTENCIALES Y ADMINISTRATIVOS,	Datos Maestros - información de usuarios	Estandares: definidos para cada una de las plantillas para el registro de datos tanto asistenciales como administrativos en los diferentes sistemas de información
	EXTRACCIÓN, TRASFORMACIÓN Y CARGA DE BASES DE DATOS			
	Gestión de Calidad de Datos Formato, completitud, codificación estandarizada para registros de Historias clínicas y datos administrativos			
COMUNICACIÓN Y OPERACIÓ	SERVICIOS DE INTEROPERABILIDAD (GEL-XML (MIN TIC) / OGC- ICDE)), facturación electrónica, nomina electrónica			
	Servicios Intercambio de		Servicios de Conectividad TI, radioenlaces de comunicaciones, fibra óptica	

PROCESOS	CERTIFICACIÓN DE OPERACIONES ESTADÍSTICAS Y/O REGISTROS ADMINISTRATIVOS
	Lenguaje Común de Intercambio – Mapas de Intercambio -- Calidad de Datos -- Estandarización con modelos de dominios sectoriales – Directorio de Componentes
FLUJOS DE INFORMACIÓN	EXTRACCIÓN TRANSFORMACIÓN Y CARGA
APLICACIONES	SISTEMAS DE INFORMACIÓN
	CNT, ENTERPRISE, IDENTIFICADOR DE USUARIOS DIGITURNO, MODULO DE VENTANILLA UNICA DE RADICACION. COMPROBADOR DE DERECHOS, PLATAFORMA ASTERIX QUE GESTIONA CALL CENTER, PAGINA WEB, INTRANET, ALMERA, SITRAD, RGISTRO DE CONSENTIMIENTOS INFORMADOS DIGITALES Y TRATAMIENTO DE DATOS PERSONALES CON FIRMAS DIGITALES

6 **ESTRATEGIA DE SEGURIDAD DIGITAL**

Salud Sogamoso E.S.E establece como estrategia de seguridad digital la que se integra a los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse acorde a la *Resolución 500 de 2021*.

Por tal motivo, *Salud Sogamoso E.S.E.* define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:



A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de los diferentes procesos de Salud Sogamoso E.S.E. del establecimiento de los roles y responsabilidades en seguridad de la información.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos MIPG.
Concientización	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.
Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

6.1 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, **Salud Sogamoso E.S..E.** define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

6.2 CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Actividades	**Responsable**	**enero**	**febrero**	**marzo**	**abril**	**mayo**	**junio**	**julio**	**agosto**	**Septiembre**	**octubre**	**noviembre**	**diciembre**
Formulacion y socialización de política de tratamiento y protección de datos personales	P. U. Recursos Informáticos, Profesional de apoyo Recursos informáticos												
Identificar los activos de información acorde al mapa de procesos institucional y realizar los registros según corresponda.	P. U. Recursos Informáticos, Profesional de apoyo Recursos informáticos												
Formulacion y socialización de política de seguridad y privacidad de la información													
Socializar y capacitar sobre el procedimiento de Gestión de Incidentes	P. U. Recursos Informáticos, Profesional de apoyo												

de seguridad de la información.	Recursos informáticos												
seguimiento a la implementación del procedimiento de reporte de incidentes de seguridad de la información	P. U. Recursos Informáticos, Profesional de apoyo Recursos informáticos												
evaluación del procedimiento de incidentes de la información según lo identificado en el indicador	P. U. Recursos Informáticos, Profesional de apoyo Recursos informáticos												
realizar estudios de costos para la adquisición e sistema de Análisis de Vulnerabilidades.	P. U. Recursos Informáticos, Profesional de apoyo Recursos informáticos												
Implementacion servidor X-ROAD servicio de interoperativodad													
Reajuste de manual de gerencia y seguridad de la información.													

lineamientos internos de ciberseguridad para proveedores y contratistas													
Formular los indicadoresde seguridad y privacidad de la informacion													

RESPONSABLES

En Salud Sogamoso se define como Líder responsable de Seguridad de la Información al Profesional Universitario de Recursos Informáticos.

Por recomendación de la "Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información" se deben desarrollar proyectos de TI y SI, para lo cual la dirección del proyecto está en manos del responsable de Sistema de Información (SI), igualmente serán responsables para la implementación los miembros del comité de gestión y desempeño en cabeza de la dirección.

6.5 APROBACIÓN

El presente plan ha sido sometido a consideración y conocimiento del comité de gestión y desempeño institucional con el objetivo de ser aprobado y aplicado conforme a lo que aquí se define.

ELABORÓ	REVISÓ	APROBÓ
Nombre CARLOS ALBERTO PARADA SUAREZ **Cargo: P.U**	Nombre: **Cargo:**	Nombre: **Cargo:** Fecha:

Documento de Referencia: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/