PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

SALUD SOGAMOSO E.S.E.

1. INTRODUCCION

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad para el año 2023

El presente plan se elabora con base al Modelo de Seguridad y Privacidad de la Información emitida por MinTIC con el fin de dar a conocer cómo se realizará la implementación y socialización del componente de Gobierno en línea en el Eje Temática de la Estrategia en Seguridad y Privacidad de la Información, el cual busca salvaguardar los datos y las historias clínicas de los pacientes en Salud Sogamoso E.S.E, garantizando la seguridad de la información.

2. DEFINICIONES

• Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

• Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

• Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

• Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

• Impacto: son las consecuencias que genera un riesgo una vez se materialice.

• Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

3. OBJETIVOS

3.1 Objetivo General: Controlar y minimizar los riesgos asociados a los procesos tecnológicos existentes, en Salud Sogamoso E.S.E con el fin de salvaguardar los

activos de información, el manejo de medios, control de acceso y gestión de usuarios.

3.2 Objetivos Específicos

• Realizar el plan de trabajo específico validando los recursos con los que se cuentan actualmente en Salud Sogamoso E.S.E para tener un plan de tratamiento de riesgo de seguridad y privacidad de la información.

• Aplicar las metodologías del DAFP e ISO 27001 asociado a seguridad y riesgo de la información.

4. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos. Junto con Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información de MINTIC.

5. POLÍTICA DE ADMINISTRACION DE RIESGOS

Salud Sogamoso E.S.E., se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes y programas, regulando los riesgos de los procesos, fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral. Opciones a tener en cuenta en la administración de los riesgos.

• Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área

• Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

• Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo

• Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

• Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros

6. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (Min TIC: 2016)

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA INICIO	FECHA FIN
Gestión de Riesgos	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Diligenciar la Matriz De Identificación, Evaluación Y Calificación De Riesgos	P.U. Recursos Informáticos	01-Feb-2023	31-Mar-2023
		Realimentación, Revisión y Revisión de los Riesgos Identificados	P.U. Recursos Informáticos. Líderes de Procesos. Control Interno	01-Abr-2023	30-Abr-2023
	Aceptación de Riesgos Identificados	Elaborar Mapa de riesgos siguiendo la Guía para la administración del riesgo y el diseño de controles en entidades públicas	P.U. Recursos Informáticos.	01-Abr-2023	30-May-2023
	Publicación	Publicación del Mapa de Riesgos	P.U. Recursos Informáticos.	01-Jun-2023	30-Jun-2023
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	P.U. Recursos Informáticos y profesional de apoyo	01-Jul-2023	30-Nov-2023
	Evaluación de Riesgos residuales	Evaluación de Riesgos residuales	P.U. Recursos Informáticos y profesional de apoyo	01-Jul-2023	30-Nov-2023
	Mejoramiento	Identificación de oportunidades de Mejora acordes a resultados	P.U. Recursos Informáticos y profesional de apoyo	01-Sep-2023	30-nov-2023

		obtenidos durante la evaluación de riesgos residuales, ajustes al plan si es necesario			
	Monitoreo y revisión	Generación, presentación y reporte de indicadores de manera bimestral	P.U. Recursos Informáticos y profesional de apoyo	01-Jul-2023	30-Nov-2023

6.1 Desarrollo Metodológico:

Análisis de la Información: En esta etapa se evaluara con los colaboradores del proceso de recursos informáticos las siguientes actividades

- Determinar los riesgos que van a ser incluidos en el plan
- Definir la herramienta para el registro y seguimiento a los riesgos identificados, causas y los efectos
- Realizar la calificación de los riesgos según la probabilidad, impacto y grado de exposición
- Determinar los controles que mitiguen los riesgo

Desarrollo de los proyectos: En esta etapa se realizaran las actividades que permitan estructurar las medidas de contención de los riesgos

- Elaboración del mapa de riesgos identificando los riesgos las causas y los efectos
- Determinar los responsables para ejecutar el tratamiento de cada riesgo identificado
- Establecer el objetivo del mapa de riesgos
- Elaborar la justificación de las medidas a tomar para mitigar los riesgos

Análisis de los proyectos

- Definir los controles a desarrollar para mitigar los riesgos
- Evaluar el impacto generado con los controles establecidos
- Validar los riesgos mitigados con cada control o medida tomada para la mitigación
- Priorizar medidas acorde al impacto generado en caso de materializar un riesgo
- Establecer si es necesario organigrama con responsabilidades respecto a la administración y gestión del riesgo.

Tratamiento de los riesgos ciclo de vida

- Definir las actividades a realizar para que los controles sean eficientes y se puedan medir por un tiempo determinado.
- Se tendrá en cuenta el ciclo PHVA para la evaluación de los riesgos e identificar las oportunidades de mejora

Recursos: En el Marco de la gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación, dispone los siguientes recursos:

- **Humanos:** El proceso de recursos informáticos de Salud Sogamoso E.S.E es el responsable de coordinar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos de la entidad en lo que concierne a la seguridad y privacidad de la información, tratamiento de datos personales. Apoyo del proceso de gestión de control interno.
- **Técnicos:** Guía de la administración del riesgo y diseño de controles para las entidades públicas, incluye los riesgos de gestión, corrupción y seguridad digital del DAFP.
- **Despliegue:** Una vez elaborado el mapa de riesgos se gestionara espacio para la socialización en comité de gestión y desempeño y luego a todos los colaboradores.
- **Financieros:** Se optimizara los recursos descritos en el presupuesto del PESI Y EL PETI según actividades descritas y asociadas a la seguridad y privacidad de la información.
- **Indicador de eficacia:** Número de controles implementados / Número de controles definidos

Documento de Referencia: Informe_Tratamiento_de_Riesgos_MINTIC.doc

ELABORÓ	REVISÓ	APROBÓ
Nombre: LAUREANO ESAU VILLAMIL LAITON **Cargo: P.U. Recursos informáticos**	COMITÉ DE GESTION Y DESEMPEÑO	COMITÉ DE GESTION Y DESEMPEÑO Fecha 27/01/2023 Acta 002