PLAN DE TRATAMIENTO Y RIESGO DE SEGURIDAD

INTRODUCCIÓN

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la ESE Hospital Materno Infantil Ciudadela Metropolitana de Soledad, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización, adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el Entorno TIC para el Desarrollo Digital, ciudadanos y hogares empoderados del Entorno Digital, Transformación Digital Sectorial y Territorial e Inclusión Social Digital. Lo anterior dando cumplimiento a la normativa establecida por el CONPES 3854 de 2016, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, adoptando las buenas prácticas y los lineamientos de los estándares ISO 27001:2013, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 emitida por el DAFP.

Gestionar eficazmente la seguridad de la información y riesgos de seguridad digital de los sistemas de información de la entidad, así como en los activos que participan en sus procesos y que se encuentran expuestos, permite garantizar la confidencialidad, integridad y disponibilidad de la información a través de la aplicación de las opciones apropiadas de tratamiento de riesgos de Seguridad de la información y seguridad digital, teniendo en cuenta la evaluación de los resultados de la valoración de los riesgos del Sistema de Gestión de Seguridad de la Información y en concordancia a la normativa aplicable. Además, con este plan se cumplirá con el objetivo de implementar controles y acciones logrando así la mitigación en los riesgos de todos los procesos de la plataforma tecnológica, reducir hallazgos de auditorías y apoya el cumplimiento del modelo integrado de planeación y gestión y a la política de gobierno digital.

OBJETIVOS

Objetivos Generales

Elaborar el plan de tratamiento y riesgo de seguridad de la información, identificado en los procesos incluidos en el modelo de seguridad y privacidad de la información de la ESE HOSPITAL MATERNO INFANTIL CIUDADELA METROPOLITANA DE SOLEDAD.

Objetivos Específicos

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los servicios en que la ESE pueda estar expuesto, y de esta manera alcanzar los objetivos, la misión y la visión institucional, protegiendo y preservando la integridad, confidencialidad, disponibilidad y autenticidad de la información.
- Calcular el nivel de riesgo
- Gestionar riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, de acuerdo con los contextos establecidos en la institución.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios de la ESE Hospital Materno Infantil Ciudadela Metropolitana de Soledad.
- Realizar seguimiento y control a eficiencia del plan de tratamiento de riesgos

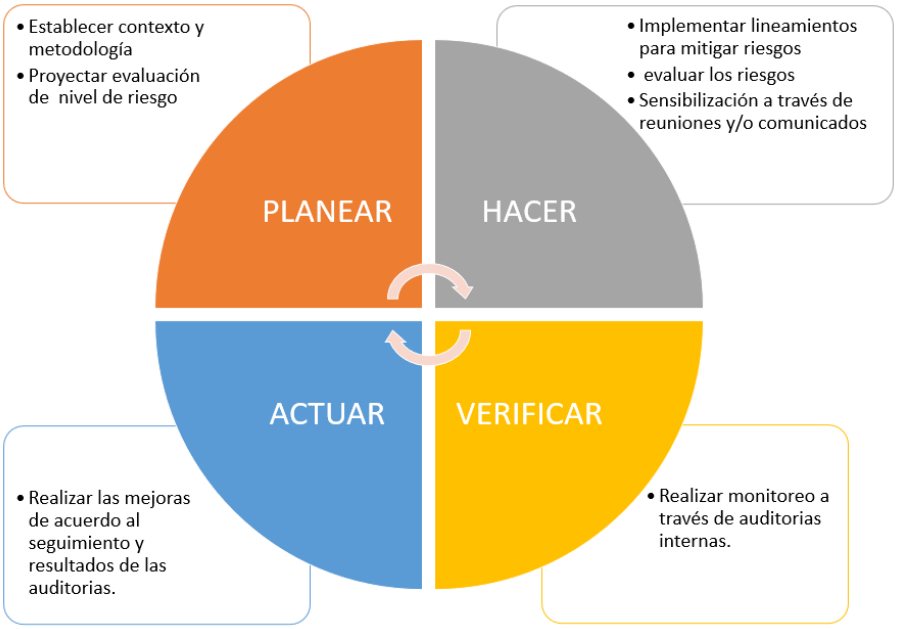
ALCANCE DEL PLAN DE TRATAMIENTO Y RIESGO DE SEGURIDAD DE LA INFORMACION

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios, 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 (MinTIC:2016)1 : se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en MINTIC. El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

DESARROLLO Y METODOLOGIA DEL PLAN DE TRATAMMIENTO Y RIESGO DE SEGURIDAD DE LA INFORMACION

El plan de tratamiento de riesgos se basará en una serie de actividades con miras a mitigar los riesgos de información, a su vez se aplicará metodologías para el análisis de los riesgos identificados para los activos de información en el que nos permita orientar y comprender claramente el nivel de riesgo a los que está expuesto la ESE. Para ello se realizará las actividades descritas en el cuadro de acciones a ejecutar para identificar puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidades y análisis de confiabilidad.

Gestión	Actividad	Tarea	Reponsable	Fecha de Inicio	Fecha de Fin
Gestión de Riesgos	Actualizacion de lineamientos de riesgos	Actualizar politica y metodologia de gestion de riesgos	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Sensibilizacion	Socializacion Guia y Herramienta- Gestion de riesgos de seguridad y privacidad de la informacion, seguridad digital y continuidad de la Operación	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Identificacion de Riesgos de Seguridad Digital y continuidad de la Operación	Identificacion, Analisis y Evaluacion de Riesgos - Seguridad y privacidad de la Informacion, Seguridad Digital y Continuidad de la Operación	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
		Realimentacion, revision y verificacion de los riesgos identificados(Ajustes)	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Aceptacion de Riesgos Identificados	Aceptacion, aprobacion Riesgos identificados y planes de tratamiento	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Publicacion	Publicacion Matriz de riesgos- SIMIG	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificacion de evidencias	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Mejoramiento	identificacion de oportunidades de mejoras acorde a los resultados obtenidos durante la evaluacion de riesgos residuales	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31
	Monitoreo y Revision	Generacion, presentacion y reporte de indicadores	Equipo de Gestion de Riesgos	2023-03-01	2023-12-31



- Análisis de la información

  En esta fase se seleccionan los procesos incluidos en el alcance del SGSI de la ESAP y se procede a programar y a agendar a los líderes de las dependencias y grupos internos de trabajo que conforman los procesos, para la identificación de riesgos. Desarrollo de los proyectos.

- Entrevista con líderes de procesos

  Se entrevista a cada líder de dependencia o grupo, se presenta la metodología y en conjunto se procede a realizar la identificación de los riesgos sobre los activos de información, los cuales se consignan en la Matriz de Riesgos.

- Identificación y calificación de riesgo

  En esta fase, el líder de proceso evalúa el nivel de impacto vs. Probabilidad y los controles existentes para calcular el nivel de riesgo.

- Definición de responsabilidad

  En esta fase, se realizará la definición de los responsables respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por control interno y la unidad TIC teniendo en cuenta la estructura organizacional para la gestión de riesgos.

De acuerdo a los anterior, si el riesgo se ubica en una zona no aceptable, cada líder responsable de los riesgos identificados, debe definir e implementar los controles necesarios para llevar el riesgo a un nivel aceptable a través del plan ad tratamiento de riesgo.