INTRODUCCIÓN

El plan de tratamiento de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios de la administración municipal de sabaneta, 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.
Dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, 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

PLAN TRATAMIENTOS DE RIESGOS

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos de la administración municipal de sabaneta.

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

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.
- **Riesgo Inherente**: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.
- **Riesgo Residual:** nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.
- **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).
- **Impacto**: son las consecuencias que genera un riesgo una vez se materialice.
- **Posibles Consecuencias:** Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros.
- **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.
- **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.

OBJETIVOS

- 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 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.
- Cumplir con los requisitos legales y reglamentarios pertinentes a la legislación colombiana.
- 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 entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos seguridad y privacidad de la información y seguridad digital

ALCANCE

Realizar una eficiente gestión de riesgos de seguridad y privacidad de la información y seguridad digital 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.

Alcaldía de Sabaneta

CLASIFICACIÓN DE LOS RIESGOS

- **RIESGOS DE SEGURIDAD DIGITAL:** Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía municipal, la integridad territorial, los intereses municipales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

- **RIESGO ESTRATEGICO:** Se asocia con la forma en que se administra la alcaldía de Sabaneta, enfocándose en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la administración municipal.

- **RIESGO OPERATIVO:** Comprende los riegos relacionados tanto con la parte operativa como técnica, incluye riesgos provenientes de las deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

- **RIESGOS DE TECNOLOGIA:** Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporten el cumplimiento de la misión.

- **RIESGOS FINANCIEROS:** Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, depende en gran parte del éxito o fracaso de la administración municipal de Sabaneta.

- **RIESGOS DE CUMPLIMIENTO:** Se asocian con la capacidad de la entidad de cumplir con los requisitos legales, contractuales, de ética y en general con su compromiso con la comunidad.

- **RIESGOS DE CORRUPCIÓN:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

- **RIESGO DE IMAGEN O REPUTACIONAL:** Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

MARCO REFERENCIAL

POLÍTICA DE ADMINISTRACION DE RIESGOS

El objetivo de la política es establecer los parámetros necesarios para una adecuada gestión de los riesgos de gestión, corrupción, seguridad y privacidad de la información, seguridad digital y continuidad de los servicios de la administración municipal de sabaneta procurando que no se materialicen, atendiendo los lineamientos establecidos en el plan de tratamientos de riesgos orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos.

Se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC que contribuyen al desarrollo social y económico del país, al desarrollo integral de los ciudadanos y la mejora en su calidad de vida.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.
El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

- Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

- Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

- Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

- Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir,

pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite a la alcaldía de Sabaneta realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la alta dirección.

METODOLOGIA

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 (MinTIC:2016)

Gestión	Actividad	Tarea	Responsable
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	Equipo de gestión de riesgos
	Sensibilización	Socialización guía y herramienta, gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de gestión de riesgos
	Identificación de riesgos y seguridad de la información, seguridad digital y continuidad de la operación	Identificación, análisis y evaluación de riesgos y seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Equipo de gestión de riesgos
		Realimentación, revisión y verificación de los riesgos identificados	
	Aceptación de riesgos identificados	Aceptación, aprobación de riesgos identificados y planes de tratamientos	Equipo de gestión de riesgos

	Publicación	Publicación matriz de riesgos	Equipo de gestión de riesgos
	Seguimiento fase de tratamiento	Seguimiento estado de planes de tratamientos de riesgos identificados y verificación de evidencias	Equipo de gestión de riesgos
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Equipo de gestión de riesgos
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de gestión de riesgos
		Actualización guía de gestión de riesgos, seguridad de la información de acuerdo a los cambio solicitados	
	Monitoreo y revisión	Generación, presentación y reportes de indicadores	Equipo de gestión de riesgos

DESARROLLO METODOLÓGICO

- **Fase 1: Análisis de la información**

  En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en el Ministerio TIC.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

- **Fase 2: Desarrollo de los proyectos**

  En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.

- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

❖ **Fase 3: Análisis de los proyectos**

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

❖ **Fase 4: Definición del organigrama de responsabilidad**

En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por la alcaldía de Sabaneta teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones de la alcaldía de Sabaneta en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte de la alcaldía de Sabaneta
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

❖ **Fase 5: Ciclo de vida del tratamiento de riesgos**

Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

CONTROL DE CAMBIOS

FECHA	VERSION	DESCRIPCION DEL CAMBIO
19/01/2022	V.1	Elaboración del plan
19/12/2022	V.2	Se modifica la tabla de gestión del riesgo donde se definían las fechas de inicio y terminación de las tareas
30/01/2023	V.3	Se trabaja con grupo interdisciplinario para identificar los riesgos asociados a la oficina TIC con respecto a la norma 27001, los cuales se incluyen en la Matriz de riesgos de la administración municipal
26/01/2024	V.4	Revisión y actualización

Elaboro: Andrés Felipe García Henao
Reviso: Diego Alejandro Montoya
Aprobó: