1. OBJETIVO

Gestionar de manera efectiva y sistemática los riesgos asociados con la seguridad de la información y la tecnología de la información en la Empresa de Aseo de Bucaramanga S.A. E.S.P.
El plan busca identificar, evaluar, mitigar y controlar los riesgos para proteger los activos de información y garantizar la continuidad del negocio.

2. ALCANCE

El presente plan de Tratamiento de riesgos de la seguridad y privacidad de la información se aplica a la Empresa de Aseo de Bucaramanga S.A. E.S.P. desde su aprobación hasta la conclusión de las actividades previstas para el año 2024. Este plan está diseñado para abordar los riesgos de seguridad digital relacionados con la plataforma tecnológica y los servicios de tecnologías de información y comunicaciones que respaldan las diversas actividades del modelo de operación por procesos adoptado por la entidad.

3. DEFINICIONES Y/O ABREVIATURAS

- Activo: cualquier elemento que tenga valor para la organización.
- 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).
- Análisis del riesgo: Se estima el riesgo con el fin de proporcionar bases que logre la evaluación y la naturaleza del riesgo.
- Causa: Elemento específico que origina el evento.
- Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos (tecnológico, legal, regional, etc.).
- Contexto interno 1: Ambiente interno en el cual la organización busca alcanzar sus objetivos (gobierno, políticas, estructura organizacional, etc.).
- 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.
- Controles: Procesos, políticas y/o actividades que pueden modificar el riesgo.
- Criterios de riesgos 2: Términos de referencia frente a los cuales se evaluará la importancia del riesgo.
- Evaluación del Riesgo: Comparar los resultados del análisis de riesgo frente a los controles implementados, con el fin de determinar el riesgo final.
- Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.
- Fuente: Elemento que por sí solo o en combinación tiene el potencial intrínseco para dar lugar a riesgo; a fuente del riesgo puede ser tangible o intangible.
- Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- Identificación del riesgo 3: Se determinan las causas, fuentes del riesgo y los eventos con base al contexto el proceso, que pueden afectar el logro de los objetivos del mismo.
- Impacto: son las consecuencias que genera un riesgo una vez se materialice.
- Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al

negocio evitando cumplir con sus objetivos.

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

4. RESPONSABLE DE LA ESTRATEGIA OPERACIONAL

Será responsabilidad de la revisión anual y actualización del Plan de seguridad de la información el Profesional de sistemas – Tics, y velar porque cada componente de este, opere y generen las salidas requeridas para garantizar su operación.

5. CONDICIONES GENERALES

Según las indicaciones del Manual de Gobierno Digital, el habilitador de Seguridad y Privacidad de la Información busca que las entidades apliquen las normas de seguridad de la información en todas sus operaciones, trámites, servicios, sistemas y en general, en todos los datos, para asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información.

A pesar de esto, el Decreto Ministerial 1078 de 2015, en su Artículo 2.2.9.1.2.1, establece que la Política de Gobierno Digital se llevará a cabo a través de un esquema que incluye diferentes elementos como gobernanza, innovación pública digital, habilitadores, líneas de acción e iniciativas dinamizadoras. En particular, destaca la importancia del habilitador de Seguridad y Privacidad de la Información, según el numeral 3.2. Esto implica que las entidades deben desarrollar capacidades mediante la aplicación de normas de seguridad y privacidad en todos sus procesos, trámites, servicios, sistemas de información y activos de información para asegurar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Modelo de Seguridad y Privacidad de la Información (MSPI), emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones, indica que, si las entidades estatales lo adoptan, ayudará a mantener la confidencialidad, integridad y disponibilidad de la información. Esto se logra a través de un proceso de gestión de riesgos, generando confianza en las partes interesadas sobre la gestión efectiva de riesgos.

En el Decreto Presidencial 612 de 2018, se establecen pautas para que las entidades del Estado integren sus planes institucionales y estratégicos al Plan de Acción. En el artículo 1 de este decreto, se modifica el Decreto Presidencial 1083 de 2015, que es el Reglamento Único del Sector de Función Pública. Se agrega un nuevo artículo, el 2.2.22.3.14, que especifica la integración de los planes institucionales y estratégicos al Plan de Acción.

Dentro de estas integraciones, en los puntos 11 y 12 del numeral correspondiente, se establece como obligación anual la elaboración de dos planes específicos para cada entidad: el "Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información" y el "Plan de Seguridad y Privacidad de la Información".

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, 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.

6. NORMATIVIDAD

NORMATIVIDAD	DESCRIPCION
Decreto Ministerial 1078 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de gobierno digital y se subroga el capitulo 1 del titulo 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y comunicaciones.
Decreto Presidencial 1083 de 2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12, Seguridad Digital".
Decreto Presidencial 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".
Decreto Presidencial 767 de 2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
Resolución Ministerial 00500 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".
ISO/IEC 27001:2013	Tecnología de la información-Técnicas de seguridad- Sistemas de Gestión de la Seguridad de la Información (SGSI)- Requisitos.

7. DESCRIPCION

8.1 DESARROLLO DEL PLAN

8.1.1 IDENTIFICACION Y VALORACION DE RIESGOS

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la EMAB S.A. E.S.P.

Se emplean técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla.

El plan propuesto en este documento comprende, como se detallará más adelante, las siguientes actividades principales: establecimiento del contexto, identificación riesgos, estimación de riesgos, evaluación de riesgos, tratamiento de riesgo y aceptación del riesgo, guardando coherencia con la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública.

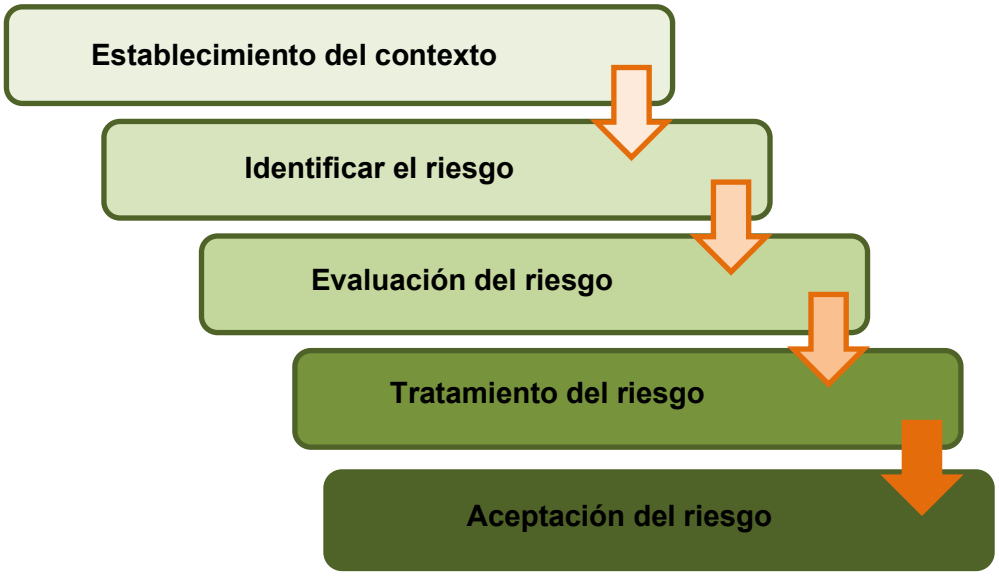

Ilustración1. Estructura general de la metodología de riesgos

La gestión del riesgo dentro de la seguridad de la información se puede también enmarcar dentro del ciclo de planear, hacer, verificar y actuar (PHVA) tal como se muestra en la siguiente ilustración (ISO 27001:2013):

Ilustración2. Ciclo PHVA y la gestión de riesgos.

La técnica de análisis de riesgo para activos de información nos permite desde un punto de vista orientado al negocio y sistémico en su naturaleza, comprender claramente los riesgos sobre los activos de información a los que puede estar expuesto la Empresa de Aseo de Bucaramanga S.A. E.S.P.
Es recomendable contar con técnicas tradicionales para identificar los riesgos específicos asociados a los activos y complementar este proceso en la medida de lo posible con la identificación de puntos críticos de fallas, análisis de disponibilidad, análisis de vulnerabilidad, análisis de confiabilidad y árboles de falla.

La Empresa de Aseo de Bucaramanga S.A. E.S.P., se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y 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.

Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

- 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.

- Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)1, las "(…) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados"(…).

8. 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 (MinTIC):

GESTION	MEDIDA	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización mapa de riesgos	Revisión y actualización de mapa de riesgos en caso de ser necesario, tener en cuenta Anexo A, ISO27001.	- Profesionales Sistemas. - Profesional Calidad	22/02/2024	31/01/2024
	Sensibilización	Socialización Plan de Tratamiento de riesgos de seguridad de la información.	Profesionales Sistemas.	31/01/2024	31/01/2024
	Identificación de riesgos de seguridad y privacidad de la información	Análisis, identificación y evaluación de riesgos - Seguridad y privacidad de la información.	Profesionales Sistemas.	26/01/2024	27/01/2024
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y plan de tratamiento.	Directora Planeación Organizacional.	31/01/2023	31/01/2023

	Publicación	Publicación matriz de riesgos, plan de tratamiento de riesgos de seguridad de la información.	Profesional Sistemas - Tics	31/01/2024	31/01/2024
	Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados - verificación de evidencias	Profesional Sistemas - OCI	1/02/2024	30/11/2024
	Mejoramiento	Identificación de oportunidades de mejora de acuerdo a los resultados obtenidos durante el seguimiento.	Identificación de oportunidades de mejora de acuerdo a los resultados obtenidos durante el seguimiento.	1/10/2024	30/11/2024
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores.	Profesional Sistemas - OCI	1/12/2024	15/12/2024

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias de la EMAB S.A. E.S.P. en este sentido.

9.1 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:

- Determinar los riesgos que se deben tratar en el mapa de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en la EMAB S.A. E.S.P.

- Fase 2: Desarrollo de las medidas

En esta fase se realizarán las actividades que permitan la estructuración de las medidas.
- Determinar el nombre de la medida.
- Definir los responsables de medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la mediad.
- Definir las tareas a realizar para el desarrollo de cada medida.

- Fase 3: Análisis de las actividades

- 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 de responsabilidad

la Dirección de Planeación Organizacional en cabeza del profesional de Tics velara por el cumplimiento de las medias establecidas formalmente en el mapa de riesgos.

- 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.

9. OPORTUNIDAD DE MEJORA

La EMAB S.A. E.S.P. no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

Con los riesgos debidamente documentados en la matriz de riesgos se busca hacer seguimiento de los mismos y garantizar la disponibilidad de la información.

10. RECURSOS

La EMAB S.A. E.S.P., en el marco de la gestión de riesgos de seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación, dispone de los siguientes recursos

RECURSOS	DESCRIPCION
Humanos	La profesional de sistemas a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua con apoyo del profesional de soporte.
Técnicos	Guía de Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 - octubre de 2018 del DAFP. - Herramienta para la gestión de riesgos (Matriz de Riesgos 2024)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de equipos, conocimiento, recursos humanos, técnicos, y desarrollo.

11. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

En el caso de que los controles impliquen la adquisición de herramienta tecnológica bajo la responsabilidad de la oficina de sistemas, los recursos de inversión.

RUBRO: TECNOLOGIA Y LICENCIAS E INFORMATICA	
OBJETO	VALOR
Renovación de la licencia del FORTINET	$ 9.500.000
Renovación del pool asignado por LACNIC para protocolo IPV6	$ 20.000.000
Licencia y soporte de correos corporativos en Gmail	$ 45.000.000
Permiso licencia sitio alterno - carrasco	$ 5.200.000
Antivirus	$ 30.000.000
Copias Azure copias en la nube	$ 2.400.000
Contrato de mantenimiento de las UPS	$ 9.800.000
Servido ICloud	$ 60.000.000
Backus equipos	$ 10.000.000
Software de seguimiento procesos judiciales	$ 2.500.000
Equipos de cómputo con licencias (10)	$ 50.000.000
Herramientas de mantenimiento sistemas	$ 80.593.136
TOTAL	$ 408.493.136

Tabla1. Presupuesto asignado a la Dirección de Planeación Organizacional para tecnología 2024.

12. SEGUIMIENTO Y CONTROL

El seguimiento y control se realizará de acuerdo a la PO-PO-001 POLITICA ADMON DEL RIESGO V.2.

13. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Creación del documento	01 de febrero de 2023
2.0	Actualización presupuesto asignado para el 2024	03 de abril del 2024