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

EMAB S.A. E.S.P.

1. ENCABEZADO

Hoy en día los diferentes factores de riesgos no sólo se pueden asociar a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos posteriores y relevantes como el terrorismo, la inestabilidad política, las pandemias y los códigos maliciosos, entre otros, han señalado la necesidad de incorporar nuevas amenazas presentes no solamente en el mundo físico sino también en el entorno digital, cuando se trate de comprender los riesgos más significativos a los activos de información.
El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis.
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.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica, hallazgos de auditorias internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC, dentro de su política de gobierno Digital.

El seguimiento al plan de tratamiento de riesgos, se realizará de acuerdo con la POLITICA DE LA ADMINISTRACION DEL RIESGO (PO-PO-001 POLITICA ADMON DEL RIESGO), diciembre 2020 y se integrará con los riesgos de seguridad digital y de la información.

2. OBJETIVOS

2.1. Objetivo general

- Disponer de la información apropiada para el desarrollo de las funciones de la EMAB S.A. E.S.P., a través de la estrategia que busca gestionar información confiable, integra y oportuna en el desarrollo de las funciones y actividades cada día.

2.2. 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 que la EMAB S.A. E.S.P. para 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 acuerdo con los contextos establecidos en la Entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación.

3. 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 se dan los lineamientos para poder identificar, analizar, tratar, evaluar y monitorear los riesgos de seguridad y privacidad de la información en la EMAB S.A. E.S.P.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles 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.

4. 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.

5. 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.

6. CONDICIONES GENERALES

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.

7. NORMATIVIDAD

NORMA	DESCRIPCIÓN
Decreto 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 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.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

8. 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.

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.
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 V4, emitida por el Departamento Administrativo de la Función Pública.

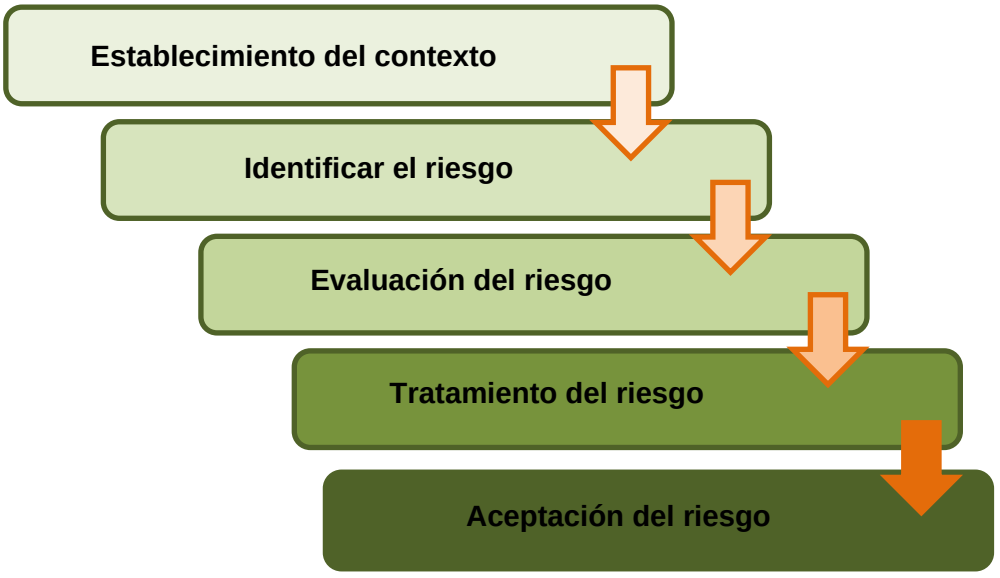

Ilustración1. Estructura general de la metodología de riesgos

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):

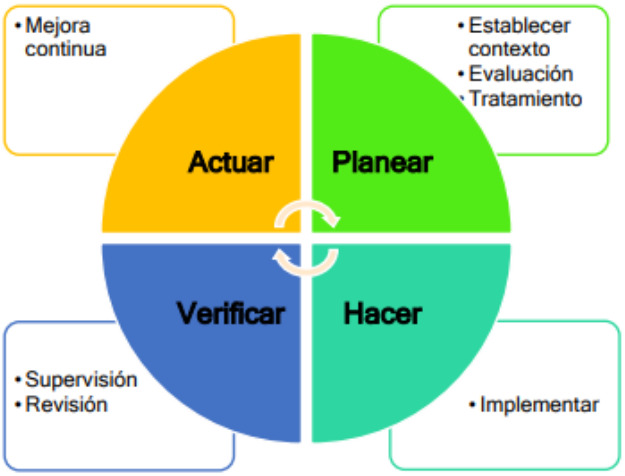

Ilustración2. Ciclo PHVA y la gestión de riesgos.

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.

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 V4, emitida por el Departamento Administrativo de la Función Pública

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.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Ministerio TIC.

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"(...).

9. 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:2016):

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
Gestión de Riesgos	Actualización mapa de riesgos	Revisión política y metodología de gestión de riesgos y actualización en caso necesario.	Profesional Calidad - Profesionales Sistemas.	26/01/2023	27/01/2023
	Sensibilización	Socialización política de gestión de riesgo y Plan de seguridad.	Profesional Calidad - Profesionales Sistemas.	1/02/2023	1/02/2023
	Identificación de riesgos de seguridad y privacidad de la información y plan de continuidad.	Análisis, identificación y evaluación de riesgos - Seguridad y privacidad de la información.	Profesional Calidad - Profesionales Sistemas.	26/01/2023	27/01/2023
	Aceptación de riesgos identificados	Aceptación, aprobación riesgos identificados y planes de tratamiento.	Director de Planeación Organizacional.	27/01/2023	27/01/2023
	Publicación	Publicación matriz de riesgos, plan de seguridad.	Profesional Sistemas - Tics	31/01/2023	31/01/2023
	Seguimiento fase de tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados - verificación de evidencias	Profesional Sistemas - OCI	1/02/2023	30/11/2023
	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.	1/10/2023	30/11/2023
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores.	Profesional Sistemas - OCI	1/12/2023	15/12/2023

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:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en la EMAB S.A. E.S.P.
- 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 EMAB S.A. E.S.P. teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones en la EMAB S.A. E.S.P. en materia de seguridad de la información.
- Definición del grupo de trabajo de gestión de riesgo por parte la EMAB S.A. E.S.P.
- 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.

10. 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

11. 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	VARIABLE
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.
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)
Logísticos	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.
Financieros	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías

12. 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.

DIRECCION DE PLANEACION ORGANIZACIONAL - 23201010030104 - TECNOLOGIA Y LICENCIAS INFORMATICAS				
Contrato Sistemas ERP Arco_Sis Plus	HORAS	1800	$ 98.400	$ 177.120.000
Licencia Antivirus (Renovar en Oct 24 2023)	UNIDAD	1	$ 3.000.000	$ 3.000.000
Servicio de Hosting Superior	UNIDAD	1	$ 600.000	$ 600.000
Servicio de Hosting	UNIDAD	1	$ 600.000	$ 600.000
Almacenamiento y análisis de datos	MES	12	$ 110.000	$ 1.320.000
Renovación de la Licencia del FORTINET	UNIDAD	1	$ 9.500.000	$ 9.500.000
LICENCIA ArcGIS para usuarios de campo (10 usuarios)	unidad	1	$ 25.000.000	$ 25.000.000
Licencias y Plataformas ArcGIS (Coordenada Urbana, ArcGIS, CIVIL 3D)	UNIDAD	1	$ 12.000.000	$ 12.000.000
Adopción de protocolo IPV4 a IPV6 FASE FINAL	UNIDAD	1	$ 20.000.000	$ 20.000.000

Desarrollo en Página Web - Implementar servicios Web	GLB	1	$ 5.000.000	$ 5.000.000
Permiso Licencia de Almacenamiento del Sitio Alterno Ubicado en El Carrasco	GLB	1	$ 5.200.000	$ 5.200.000
Licencia y Soporte de Correos Corporativos en Gmail	UNIDAD	1	$ 33.000.000	$ 33.000.000
Servicios-Copias Azure Copias en la Nube (Página Web y PQR´s)	MES	12	$ 100.000	$ 1.200.000
Certificación del Cableado de Rack en Sede Administrativa y Carrasco Marcado de Puntos Certificados	GLB	1	$ 3.000.000	$ 3.000.000
ADQUISICION DE SOFWARE PARA MANTENIMIENTO		1	$ 20.000.000	$ 20.000.000
Homologación usuarios y seguimiento de rutas		1	$ 347.000.000	$ 347.000.000
TOTAL				$ 663.540.000

Tabla1. Presupuesto asignado a la Dirección de Planeación Organizacional.

13. SEGUIMIENTO Y CONTROL

El seguimiento y control se realiza de acuerdo a la PO**-PO-001 POLITICA ADMON DEL RIESG.,** por parte del responsable de la gestión del riesgo y en por parte de la oficina de Control Interno.

14. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
1.0	Creación del documento	01 de febrero de 2023