Nombre de la política / plan:	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
Dependencia responsable:	Subdirección Administrativa y Financiera Área de apoyo tecnológico de la información
Fecha de aprobación de la política / plan:	ENERO 30 DE 2024
No. de acta del Comité Institucional de Gestión y Desempeño del AMB en que fue aprobada:	Acta N° 01
Vigencia de la política / plan:	2024
Dimensión del MIPG a la que se asocia la política / plan:	Información y Comunicación

Plan 2024

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

Apoyo Tecnológico
SUBDIRECCÓN ADMINISTRATIVA Y FIANNCIERA

Contenido

INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información establece las actividades requeridas para la gestión de los riesgos de seguridad y privacidad de la información, en función de la implementación de controles que permitan a la entidad disminuir la probabilidad y el impacto de materialización de este tipo de riesgos, con el fin de preservar la seguridad e integridad de los activos de información de la Entidad.

El Área Metropolitana de Bucaramanga AMB como entidad Pública busca afrontar los diferentes retos con una infraestructura moderna, robusta y segura, que sea competitiva en el nuevo mundo digital. Por ello La gestión de la seguridad de la información debe realizarse sistemáticamente por procesos completamente documentados y conocidos por toda la entidad.

Con ello se busca promover la implementación y ejecución de buenas prácticas de seguridad y privacidad de la información que constituyen un SGSI que podría llegar a llamarse como un sistema de calidad para la seguridad de la información, teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información del Ministerio de las TIC.

1. OBJETIVOS

1.1 Objetivo general

Identificar y dar prioridad a todas las actividades contempladas en el presente documento “PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÒN DEL AMB 2018 – 2020”, alineados con la Política de Gobierno Digital (Estrategia de MINTIC) con fin de Mitigar oportunamente los riesgos asociados a la seguridad y privacidad de la información del Área Metropolitana de Bucaramanga y que las personas interesadas tengan la confianza en el tratamiento de la información que realiza la entidad.

Continuar con la implementación, desarrollar y seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, de acuerdo con lo establecido en el Modelo de Privacidad y Seguridad de la Información – MSPI, la Guía de Gestión de Riesgos y la Guía de Controles de Seguridad y Privacidad de la Información, con el propósito de adoptar medidas y acciones encaminadas a modificar, reducir o eliminar riesgos relacionada con la infraestructura de tecnologías de la Información de la Entidad.

1.2 Objetivos específicos

- Actualizar los posibles riesgos a los que se encuentra expuesta la entidad en materias de seguridad y privacidad de la información.

- Valorar los riesgos a los cuales se encuentra expuesta la información.

- Socializar a todos los colaboradores, áreas, procesos, proveedores externos con los que se intercambia o procesa información, sobre la necesidad e importancia de gestionar de manera adecuada políticas que minimicen perdida, alteración o tiempos de entrega en la gestión.

- Involucrar y comprometer a todos en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos.

- Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional.

- Planificar el tratamiento de cada uno de los riesgos hallados.

1.3 Objetivos estratégicos

Actualizar el plan de tratamiento de riesgos que hace parte complementaria del plan de gestión de seguridad y privacidad de la información y de esta manera mitigar todos los riesgos hallados enla fase de Diagnostico o cualquier otro que se pueda generar, en el desarrollo de las áreas misionales de la entidad.

2. ALCANCE DEL PLAN

El alcance del presente plan comprende todas las actividades que permitan dar cumplimiento de los componentes definidos en esta etapa de seguimiento, continuidad y planeación en el Modelo deriesgos de la Seguridad y Privacidad de la Información del Ministerio de las Tics.

.

3. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Aceptación del riesgo:** decisión de asumir un riesgo [Fuente 3.1 ISO/IEC 27001]

- **Activo:** Cualquier cosa que tiene valor para la organización [Fuente 3.2 ISO/IEC 27001] Gestión de Riesgos de Seguridad de la Información se consideran los siguientes tipos: información, actividades y procesos del negocio, software, hardware, personal, redes, organización y ubicación.

- **Amenaza**: situación externa que no controla la entidad y que puede afectar su operación

- **Análisis de riesgo:** uso sistemático de la información para identificar las fuentes y estimar el riesgo. [Fuente 3.3 ISO/IEC 27001]

- **Confidencialidad:** Propiedad que determina que la información no esté disponible ni sea revelada a individuos o entidades no autorizados. [Fuente 3.4 ISO/IEC 27001]

- **Causa:** medios, circunstancias y/o agentes que generan riesgos.

- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.

- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [Fuente 3.6 ISO/IEC 27001]

- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.

- **Evaluación del riesgo:** Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Fuente 3.7 ISO/IEC 27001]
- **Gestión del Riesgo**: Actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Fuente 3.9 ISO/IEC 27001]

- **Incidente de seguridad de la información**: Un evento o serie de eventos de seguridad de la información no deseado o inesperado, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [Fuente 3.10 ISO/IEC 27001]

- **Integridad:** Propiedad de salvaguardad la exactitud y estado completo de los activos [Fuente 3.11 ISO/IEC 27001]

- **Riesgo:** Efecto de incertidumbre sobre los Objetivos. [Fuente ISO 31000]

- **Riesgo Residual:** Nivel relevante del riesgo después del tratamiento del riesgo. [Fuente 3.12 ISO/IEC 27001]

- **Riesgo de corrupción**: posibilidad de que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.

- **Riesgo inherente**: es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.

- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio

- **Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información, además puede involucrar propiedades como: autenticidad, trazabilidad, no repudio y fiabilidad.

4. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

El éxito de la administración del riesgo depende de la decidida participación de los directivos, servidores públicos y contratistas; por esto, es preciso identificar los actores que intervienen:

- Alta Dirección:

  aprueban las directrices para la administración del riesgo en la Entidad. La alta Dirección es la responsable del fortalecimiento de la política de administración del riesgo.

- Proceso Administración del Sistema Integrado de Gestión:

  Genera la metodología para la administración del riesgo de la Entidad, coordina, lidera, capacita y asesora en su aplicación.

- Responsables de los procesos:

  Identifican, analizan, evalúan y valoran los riesgos de la entidad (por procesos e institucionales) al menos una vez al año.

- Servidores públicos y contratistas:

Ejecutar los controles y acciones definidas para la administración de los riesgos definidos, aportar en la identificación de posibles riesgos que puedan afectar la gestión de los procesos y/o de la entidad.

- Quien haga las veces de Control Interno:

  Debe realizar evaluación y seguimiento a la política, los procedimientos y los controles propios de la administración de riesgos.

5. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO

En el área metropolitana de Bucaramanga, AMB adelantará las acciones pertinentes para la implementación y mantenimiento del proceso de Administración del Riesgo de la seguridad y privacidad de la información, y para ello todos los servidores de la entidad se comprometen a:

1. Gestión de recursos necesarios para implementación de nuevos esquemas para prevenir el riesgo de la seguridad y privacidad de la información en el AMB.

2. Dar a Conocer a todos los funcionarios del área metropolitana de Bucaramanga y hacer cumplir las normas internas y externas relacionadas con la administración de los riesgos.

3. Fortalecer dentro de la institución la cultura de administración de los riesgos para crear conciencia colectiva sobre los beneficios de su aplicación y los efectos nocivos de su desconocimiento.

4. Reportar los eventos de riesgo que se materialicen, utilizando los procedimientos e instrumentos establecidos para el efecto.

5. Presentar propuestas de mejora continua que permitan optimizar la forma de realizar y gestionar las actividades de la entidad para así aumentar nuestra eficacia y efectividad.

Para lograr lo anteriormente enunciado dependemos de una aprobación de recursos tanto humanos como presupuestales y tecnológicos necesarios, por parte de la Alta Dirección que permitan realizar el seguimiento y evaluación a la implementación y efectividad de esta política.

De igual manera, la presente guía forma parte de la política de administración del riesgo, por cuanto detalla las directrices que deben tenerse en cuenta para la gestión del mismo en la entidad y que tienen como propósito evitar la materialización del riesgo.

6. ETAPAS PARA LA ADMINISTRACIÓN DEL RIESGO

Las etapas a desarrollar durante la administración del riesgo; en la descripción de cada etapa se desplegarán los aspectos conceptuales y operativos que se deben tener en cuenta.

- Contexto estratégico: Actualizar los factores externos e internos del riesgo.
- Identificación: Actualizar la identificación de causas, riesgo, consecuencias y clasificación del riesgo.
- Análisis: Actualizar la calificación y evaluación del riesgo inherente.
- Valoración: Actualizar la identificación y evaluación de controles; incluye la determinación del riesgo residual.
- Manejo: determinar, si es necesario, acciones para el fortalecimiento de los controles.
- Seguimiento: evaluación integral de los riesgos.

7. CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD	TAREA A DESARROLLAR PARA EL PLAN	RESPONSABLE	FECHA INICIAL PLANIFICADA (dd-mm-aa)	FECHA FINAL PLANIFICADA (dd-mm-aa)
Actualizar el inventario de activos de información (software y hardware)	Actualizar el inventario actual de todos los activos de TIC de software y hardware	Área de apoyo tecnológico y de la información	MARZO 2024	MAYO 2024
Actualizar e identificar nuevos riesgos de seguridad y privacidad de la información, Seguridad Digital y continuidad de la Operación	Identificación, Análisis y evaluación de riesgos- Seguridad y privacidad de la información, Seguridad Digital y continuidad de la operación	Área de apoyo tecnológico y de la información	MARZO 2024	JUNIO 2024
Implementar controles de seguridad de la información para abordar los riesgos de seguridad y privacidad de la información identificados, analizados, valorados y priorizados sobre los activos de información	Elaborar y/o actualizar políticas según el modelo de Seguridad y Privacidad de la Información, el plan de tratamiento de riesgos	Área de apoyo tecnológico y de la información	JUNIO 2024	AGOSTO 2024
Socialización de controles de Seguridad y Privacidad de la Información y gestión de riesgo	Socializar políticas y documentos	área de apoyo tecnológico y de la información	AGOSTO 2024	AGOSTO 2024

8. DOCUMENTOS DE REFERENCIA

- MPSI Modelo de Seguridad y Privacidad de la Información del Ministerios de las TIC
- ISO 27001:2013 Norma internacional emitida por la Organización Internacional de Normalización(ISO) sobre gestión de seguridad de la información.
- LEY 1581:2012 Por la cual se dictan disposiciones generales para la protección de datos personales.
- 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.

- Decreto 1078 de 2015 Decreto Único Reglamentario del sector de Tecnologías de la Informacióny las Comunicaciones.

9. MARCO LEGAL

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data y Artículo 20. Libertad de Información.
- Decreto 612 de 4 de abril 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 1008 de 14 de junio de 2018, Por el cual se establecen los lineamientos generales de la política de Gobierno Digital

10. REQUISITOS TECNICOS

- Norma técnica colombiana NTC ISO/IEC 27001:2013 Sistemas de Gestión de la seguridad de la información.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Artículo de gestión del riesgo, Ministerio de Tecnologías y Sistemas de Información.

Elaboró

Ing. Freddy Neil Varela Lemus. PU – SAF