Nombre de la política / plan:	PLAN 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:	28 enero del 2025
No. de acta del Comité Institucional de Gestión y Desempeño del AMB en que fue aprobada:	Acta numero 1
Vigencia de la política / plan:	2025
Dimensión del MIPG a la que se asocia la política / plan:	Información y Comunicación

Plan 2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SUBDIRECCÓN ADMINISTRATIVA Y FIANNCIERA
Apoyo Tecnológico y de Información

Contenido

INTRODUCCIÓN

El AREA METROPOLITANA DE BUCARAMANGA identifica la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones, en la gestión de los procesos continuamente se está gestionando, almacenando, procesando, custodiando, transfiriendo e intercambiando información valiosa que no debe ser divulgada a personal no autorizado, suceso que puede poner en riesgo la gestión pública. La defensa y protección de los activos de información es una tarea esencial para asegurar la continuidad y el desarrollo de los objetivos institucionales, asimismo garantiza el cumplimiento normativo aplicable a la Entidad, y refuerza la confianza de las partes interesadas.

La normativa establece que el proceso de Seguridad y Privacidad de la Información debe alinearse con el habilitador de seguridad y privacidad de la información contemplado en la Política de Gobierno Digital, tal como lo dispone el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones". Este artículo obliga a los sujetos regulados a desarrollar capacidades mediante la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información. El propósito de estas disposiciones es garantizar la preservación de la confidencialidad, integridad, disponibilidad y privacidad de los datos, asegurando así una gestión adecuada de la información y el cumplimiento de las obligaciones normativas.

Ahora bien, el Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública", establece en su artículo 16 que "las autoridades que realicen trámites, procesos y procedimientos por medios digitales deberán disponer de sistemas de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información". Por lo tanto, es fundamental implementar una estrategia de seguridad digital que siga los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones, garantizando así el cumplimiento normativo y la protección de los datos gestionados por medios electrónicos.

La Resolución 500 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", que forma parte de la Política de Gobierno Digital reglamentada por el Decreto 1078 de 2015, dispone que las entidades señaladas en el artículo 2.2.9.1.1.2 del mencionado decreto son sujetos obligados a cumplir con dicha política. En consecuencia, estas entidades deben definir lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), incluyendo la gestión de riesgos de seguridad de la información, el procedimiento para la gestión de incidentes de seguridad digital y los lineamientos y estándares que orienten la estrategia de seguridad digital. Este marco busca garantizar una gestión integral de la seguridad y privacidad de la información en cumplimiento con los objetivos de la Política de Gobierno Digital.

En atención a lo anterior y siguiendo los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG, se establece el Plan de acción de Seguridad y Privacidad de la Información del AMB para la vigencia 2025, que define la hoja de ruta de la estrategia de seguridad digital para gestionar y proteger la información suministrada

a la Entidad y generada por la misma de las diferentes amenazas que pueden afectar la integridad, disponibilidad, confidencialidad y privacidad de la información; mediante la planeación de actividades para la mejora continua del Sistema de Gestión de Seguridad Digital – SGSD y del Programa Integral de Protección de Datos Personales.

OBJETIVOS

GENERAL

Establecer las acciones a desarrollar durante la vigencia 2025, en el marco de la actualización del Sistema de Gestión de Seguridad de la Información – SGSI institucional, alienadas al Modelo de Seguridad y Privacidad de la Información – MSPI de la política de Gobierno Digital del MinTIC, la NTC/IEC ISO 27001, la Política pública de Seguridad Digital, y los criterios de Continuidad de la operación de los servicios, que permitan mantener la seguridad y privacidad de la información que circula en los procesos del Área Metropolitana de Bucaramanga

ESPECÍFICOS

- Ejecutar el ciclo de mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI), mediante la actualización de los instrumentos, procesos y procedimientos institucionales de seguridad de la información, en procura del fortalecimiento y optimización de la gestión de seguridad y privacidad de la información en la entidad.
- Gestionar de manera efectiva los riesgos de seguridad de la información de la AMB
- Propender por la apropiación en todos los colaboradores de la entidad, de una cultura de seguridad de la información.
- Implementar y optimizar controles técnicos, que permitan fortalecer la seguridad digital y ciberseguridad en la AMB.

ALCANCE

El Plan de acción de Seguridad y Privacidad de la Información, aplica a todo el modelo de operación por procesos de la entidad, contempla las actividades requeridas por la normativa en la materia, la atención a las necesidades de las áreas en temas de seguridad y privacidad de acuerdo con el Modelo de Seguridad y Privacidad del MAB, la Políticas de Seguridad Digital y el Programa Integral de Protección de Datos Personales.

MARCO NORMATIVO

- Ley 1581 de 2012– Protección de Datos Personales.
- Ley 1712 de 2014– Transparencia y Derecho de Acceso a la Información Pública.
- Ley 2088 de 2021. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.
- Ley 2052 de 2020. Por medio de la cual se expide el código general disciplinario.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- 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 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 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 2106 de 2019, establece la disposición de una estrategia de seguridad digital acorde con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones- MInTic.
- Decreto 1377 de 2013 (Compilado en el Decreto 1081 de 2015), por el cual se reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 103 de 2015, por el cual se reglamenta parcialmente la Ley 1712 de 2014 y el acceso a la información pública.
- Decreto 886 de 2014, Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
- Decreto 1008 de 2018 – Política de Gobierno Digital (MinTIC).
- Decreto 338 de 2022, contiene lineamientos generales para fortalecer la gobernanza de la seguridad digital.
- MINTIC: Modelo de Seguridad y Privacidad Digital (MSPI) de la Estrategia de Gobierno Digital.
- NTC-ISO-IEC 27001 – norma técnica colombiana – Sistema de Gestión de Seguridad de la Información.
- Modelo Integrado de Planeación y Gestión – Dimensión Seguridad Digital.
- CONPES 3701 de 2011 - Estrategia de Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016 Política Nacional de Seguridad digital
- CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital.
- Directiva presidencial 03 de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.
- Directiva presidencial 02 de 2022. Lineamientos para el uso de servicios en la nube, actualización de catálogos de servicios, sistemas de información, bases de datos, activos de información, infraestructura; Implementar una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos, conformación de un equipo o Grupo de Seguridad Digital.
- Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.
- Resolución 500 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"
- Resolución 1519 de 2020. Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos".
- Resolución 460 de 2022 "Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación".
- Superintendencia de Industria y comercio: Circular externa 002 de 2024, establece lineamientos específicos para el tratamiento de datos personales en sistemas de inteligencia artificial (IA).

DEFINICIONES

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.
- Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- Seguridad de la información Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).
- Sistema de Gestión de Seguridad de la Información SGSI Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
- Vulnerabilidad Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

DESARROLLO DEL PLAN

A continuación, se relaciona el cronograma de actividades del Plan de Acción de Seguridad y Privacidad de la Información para el año 2025:

Para definir las actividades del presente plan se analizó la situación actual vs la deseada, buscando en todo momento una alineación con la normativa de seguridad y privacidad de la información. A continuación, se ilustra el análisis para la definición del Plan de Acción de Seguridad y Privacidad de la Información para el año 2025:

Situación actual:

Dentro de las revisiones a algunos controles específicos de la norma ISO27001, se ha identificado necesidades de fortalecer la efectividad y diseño de estos, toda vez que no garantizan la debida protección a la información, siendo necesario continuar generando verificaciones a todo el Sistema de Gestión de Seguridad Digital y se logren medidas mitigantes de los riesgos de seguridad de la información. Respecto a los resultados del FURAG

del año 2023, donde se obtuvo un puntaje de 35.8% para la Política de Seguridad Digital, encontrando un indicador en el que se debe actuar de manera inmediata para lograr fortalecer esta Política y lograr mejorar los resultados en la medición, garantizando la seguridad y privacidad de la información de la entidad.

Situación deseada:

El Sistema de Gestión de Seguridad Digital como proceso transversal propende apoyar el logro de las metas institucionales, aportando desde la perspectiva de seguridad digital en todos los procesos y proyectos en los que se encamine la Entidad.

Como segundo aspecto, procura dar estricto cumplimiento a las políticas y procedimientos de seguridad digital, bajo un enfoque de sensibilización y concienciación de todas las partes interesadas, destacando el compromiso de la alta dirección con las estrategias de seguridad de la información.

En tercer lugar, espera contar con un esquema robusto de monitoreo y respuesta a incidentes de seguridad digital que permita actuar adecuadamente y minimizar el impacto en la Entidad. También se deben cerrar las brechas en la implementación de controles, que puedan mitigar el riesgo a la afectación de la información pública y privada, protegiendo la privacidad de la información en todas las dependencias.

Cronograma

A continuación, se relacionan el cronograma de actividades del Plan de Acción de Seguridad y Privacidad de la Información para el año 2025:

Actividad	Responsable de la Tarea	Evidencia	Fechas Programación Tareas	
			Fecha Inicio	Fecha Final
Contratación del personal con experiencia acreditada en Seguridad y Privacidad de la Información	Secretaria General Subdirección Administrativa y Financiera	Contrato	01-feb-25	31-mar-25
Revisar y actualizar la Política de seguridad y privacidad de la información	Secretaria General Subdirección Administrativa y Financiera	Política actualizada	01-abr-25	31-may-25
Difundir la política de seguridad y privacidad de la información mediante campañas institucionales	Secretaria General Subdirección Administrativa y Financiera	Socializar política	01-jun-25	05-jun-25
Autodiagnóstico de Modelo de Seguridad y Privacidad de la Información (MSPI) de Mintic	Secretaria General Subdirección Administrativa y Financiera	Informe Formato MinTic	01-abr-25	30-jun-25
Actualizar y consolidar los activos de información y socializarlo	Secretaria General Subdirección Administrativa y Financiera	Informe	01-abr-25	31-jul-25

Actualizar y consolidar el catálogo de activos de información y socializarlo	Secretaria General Subdirección Administrativa y Financiera	Informe	01-abr-25	31-jul-25
Actualizar los riesgos de seguridad sobre activos de información	Secretaria General Subdirección Administrativa y Financiera	Informe	01-ago-25	31-ago-05
Definir roles y responsabilidades	Secretaria General Subdirección Administrativa y Financiera	Informe	01-ago-25	31-ago-25
Sensibilización y capacitación en seguridad de la información	Secretaria General Subdirección Administrativa y Financiera	Capacitación	01-abr-25	15-sep-25
Gestionar la implementación de controles de seguridad	Secretaria General Subdirección Administrativa y Financiera	Informe	01-abr-25	30-nov-25

Recursos

Humanos

Se requiere la contratación de personal con experiencia acreditada en la implementación de modelos de seguridad y privacidad de la información – MinTic – ISO 27001

Seguimiento y evaluación:

Con el fin de garantizar un seguimiento y evaluación al plan de acción, se establece los siguientes indicadores:

- Apropiación en Seguridad Digital = (Número de funcionarios capacitados / Número total de funcionarios convocados) *100
- % Cumplimiento Plan de Acción = Nº Actividades Ejecutadas / Nº Actividades Planificadas

Elaboró

Ing. Freddy Neil Varela Lemus.
Profesional Universitario
Subdirección Administrativa y Financiera