

2025

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



ALCALDÍA DE
BUCARAMANGA

Caja de
Previsión Social
Municipal

CPSM

Versión 0

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CAJA DE PREVISIÓN SOCIAL MUNICIPAL DE BUCARAMANGA

Dirección General
Alejandra Serrano R.

Gestión de Tecnologías de Información
Jhonatan Tique Marín


Gestión de Calidad
Liliana M. Delgado Castellanos

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN		Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		Versión: 0	Pág. 1 11
			Fecha Aprobación: 30/01/2025	

TABLA DE CONTENIDO

1. OBJETIVO	2
1.1 OBJETIVOS ESPECÍFICOS	2
2. ALCANCE.....	2
3. MARCO NORMATIVO	3
4. CONTEXTO INSTITUCIONAL.....	4
4.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.....	4
4.2 ESTRATEGIA DE SEGURIDAD DIGITAL	5
4.3 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES).....	6
5. ACTIVIDADES ASOCIADAS AL PLAN DE SEGURIDAD DE LA INFORMACIÓN	8

COPIA CONTROLADA

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 2 11
		Fecha Aprobación: 30/01/2025	

1. OBJETIVO

Definir la estrategia del Plan de Seguridad y Privacidad de la Información para el período 2025 de la CPSM. El propósito principal del Plan de Seguridad de la Información es proteger la información institucional a través de una gestión de riesgos eficiente y la aplicación de controles adecuados.

Este plan está diseñado para garantizar la confidencialidad, integridad y disponibilidad de los activos de información que respaldan los procesos de la entidad, estableciendo un entorno seguro y controlado frente a amenazas y vulnerabilidades potenciales.

1.1 OBJETIVOS ESPECÍFICOS

Garantizar la alineación de la estrategia de Seguridad de la Información con las metas y objetivos institucionales de la CPSM.

Diseñar y ejecutar iniciativas y actividades que aseguren el cumplimiento efectivo de la estrategia de Seguridad de la Información.


Establecer medidas técnicas, administrativas y de gestión del talento humano orientadas a la implementación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI).

Planificar el seguimiento, la medición y el análisis de los controles implementados para la adopción efectiva del MSPI.

Asegurar el respaldo y compromiso de la Dirección mediante el fortalecimiento y apoyo constante a las actividades y acciones destinadas a la implementación del MSPI.

2. ALCANCE

Este plan abarca todos los procesos, el recurso humano y de manera general, cada activo de información que sustenta las operaciones internas de la CPSM. Su implementación efectiva está estrechamente alineada con el alcance definido en la Política de Seguridad de la Información, así como

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 3 11
		Fecha Aprobación: 30/01/2025	

con las directrices establecidas en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) adoptado por la entidad.

Este enfoque estratégico asegura que las medidas de seguridad aplicadas sean coherentes con las mejores prácticas, los marcos normativos y los estándares relevantes, fortaleciendo la protección integral de los activos institucionales.


3. MARCO NORMATIVO

El Plan Estratégico de Seguridad y privacidad de la Información se fundamenta en una sólida base de documentos, normas y lineamientos que orientan su estructura y funcionamiento. Estos incluyen políticas internas, marcos normativos nacionales e internacionales, estándares reconocidos de gestión de seguridad de la información, así como guías y procedimientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI). Esta integración asegura una alineación consistente con las mejores prácticas y requisitos legales, proporcionando un enfoque robusto y efectivo para la protección de los activos de información de la CPSM.

Decreto Nacional 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 746 de 2022 expedida por el Ministerio de TIC, "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021"

Guía DAFP Guía para la Administración del Riesgo, "Guía para la Administración del Riesgo y el diseño de controles en entidades públicas (Versión 6)"

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 4 11
		Fecha Aprobación: 30/01/2025	

Decreto Nacional 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”

Plan de Seguridad de la Información como uno de los requisitos a desarrollar para cumplir con esta normativa.

Resolución 500 de 2021 expedida por el Ministerio de TIC, “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”.

CONPES 3995 de 2020, “Política Nacional de Confianza y Seguridad digital”

Manual de Gobierno Digital – MINTIC

Modelo de Seguridad y Privacidad de la Información – MINTIC


Ley Estatutaria 1581 de 2012. Ley de Protección de Datos Personales

4. CONTEXTO INSTITUCIONAL

4.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El propósito central de este autodiagnóstico es realizar una evaluación exhaustiva de la eficacia de las medidas de seguridad implementadas, identificando áreas de mejora y oportunidades de fortalecimiento.

Este análisis integral abarca todos los procesos y activos de información de la CPSM, con el fin de detectar de manera proactiva cualquier vulnerabilidad o riesgo potencial que pueda comprometer la seguridad de los activos de información y la infraestructura tecnológica.

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 5 11
		Fecha Aprobación: 30/01/2025	

4.2 ESTRATEGIA DE SEGURIDAD DIGITAL

El objetivo central de esta estrategia es garantizar la protección integral de la información, la infraestructura tecnológica y los activos de información de la CPSM, con especial énfasis en salvaguardar la confidencialidad, integridad y disponibilidad de los datos institucionales.

La estrategia se fundamenta en un enfoque proactivo de gestión de riesgos en seguridad de la información, respaldado por la implementación de controles efectivos para mitigar riesgos de manera adecuada.

Asimismo, se definirán acciones específicas para la gestión oportuna y eficiente de incidentes de seguridad digital, fomentando una sólida cultura de seguridad de la información que potencie las capacidades de los usuarios y terceros vinculados a la entidad.

Adicionalmente, se implementarán medidas orientadas a la protección de los datos de los ciudadanos, reforzando el compromiso de la CPSM con la prestación de servicios seguros y confiables a través de las Tecnologías de la Información y las Comunicaciones. Este enfoque busca no solo cumplir con los estándares de seguridad, sino también consolidar un ecosistema digital basado en la confianza, la transparencia y la continuidad operativa.

En línea con estos objetivos, se han definido cinco estrategias específicas que, en conjunto, permitirán estructurar una estrategia general de seguridad digital orientada a fortalecer la protección y resiliencia de la CPSM.


	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 6 11
		Fecha Aprobación: 30/01/2025	




4.3 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se presenta el propósito de cada estrategia específica a implementar, garantizando que las actividades estén alineadas con los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 500 de 2021 emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC):

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Liderazgo de seguridad de la información	Asegurar el respaldo de la Alta Dirección, representada en el Comité Institucional de Gestión y Desempeño. El respaldo y compromiso de la Alta Dirección es esencial para alcanzar con éxito los objetivos establecidos en la adopción, mantenimiento y mejoramiento continuo del Modelo de

	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN		Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		Versión: 0	Pág. 7 11
			Fecha Aprobación: 30/01/2025	

	<p>Seguridad y Privacidad de la Información (MSPI) en nuestra entidad.</p> <p>El apoyo de la Alta Dirección y de los líderes de los diferentes procesos de la Entidad fortalece la toma de decisiones estratégicas y la asignación de recursos necesarios para la implementación efectiva de las iniciativas, así como el establecimiento de roles y responsabilidades relacionadas con la seguridad de la información.</p>
Gestión de riesgos	<p>Establecer lineamientos claros para la identificación, análisis, valoración y tratamiento de los riesgos de seguridad de la información asociados con todos los activos de la entidad.</p> <p>La implementación de la administración de riesgos de seguridad de se centrará en orientar la ejecución de controles, así como acciones preventivas y correctivas con el propósito de anticipar eventos no deseados que puedan impactar negativamente en el logro de los objetivos institucionales.</p> <p>Esta estrategia no solo busca mitigar riesgos, sino también establecer un marco proactivo que fortalezca la resiliencia de la entidad frente a posibles amenazas a la seguridad de la información.</p>
Concientización	<p>Consolidar una cultura organizacional de seguridad de la información al interior de la entidad definiendo un marco de comportamiento enfocado a la implementación de buenas prácticas alrededor de la seguridad y el control frente al tratamiento de la información de la compañía.</p>
Implementación de controles	<p>Desarrollar diversos mecanismos para la implementación de controles necesarios con el fin de garantizar los más altos niveles de seguridad para los diversos activos de información de la entidad.</p>


	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Versión: 0	Pág. 8 11
		Fecha Aprobación: 30/01/2025	

	Estos mecanismos se diseñarán y desplegarán estratégicamente para asegurar la confidencialidad, integridad y disponibilidad de la información institucional.
Gestión de incidentes	Definir mecanismos que permitan establecer una hoja de ruta para responder de forma adecuada y oportuna frente a posibles eventos de seguridad adversos que puedan afectar los activos de información críticos de la Entidad, buscando mitigar la pérdida de información y/o la interrupción de los servicios tecnológicos que soportan los diferentes procesos al interior de la entidad.


5. ACTIVIDADES ASOCIADAS AL PLAN DE SEGURIDAD DE LA INFORMACIÓN

La CPSM define las siguientes actividades con el propósito de avanzar en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

ESTRATEGIA / EJE	ACTIVIDAD	PRODUCTOS ESPERADOS
Liderazgo de la seguridad de la información	Hacer Seguimiento, monitoreo y actualización a las políticas, manuales, procedimientos, guías, formatos, entre otros asociados a Modelo de Seguridad y Privacidad de la Información (MSPI).	Informe de Políticas definidas y aprobadas en el comité de gestión y desempeño MIPG
	Diseñar y ejecutar los proyectos que permitan la correcta implementación de las actividades y estrategias de seguridad de la información al interior de la entidad.	Implementación de proyectos asociados a Seguridad de la información y Ciberseguridad ejecutados al interior de la entidad.

 <p>ALCALDIA DE BUCARAMANGA Caja de Previsión Social Municipal</p>	PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN		Código: GTI-P003
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		Versión: 0
			Pág. 9 11
			Fecha Aprobación: 30/01/2025

Gestión de riesgos	Hacer Seguimiento, monitoreo y actualización al mapa de riesgos de seguridad de la información	Inventario de activos de información actualizado.
	Hacer Seguimiento, monitoreo y actualización al inventario de activos de información.	Mapa de Riesgos de Seguridad de la Información actualizado.
	Diseño de una estrategia que permita hacer seguimiento al Plan de tratamiento de riesgos de seguridad de la información de la entidad.	Informe de seguimiento al Plan de Tratamiento de Riesgos de Seguridad de la Información
Concientización	Diseñar una estrategia de capacitación, sensibilización y concientización en temas relacionados con la seguridad y privacidad de la información, dirigido a funcionarios, contratistas y personal de nivel directivo	Plan de capacitación y Sensibilización
		Informe con los resultados obtenidos durante los ejercicios y campañas realizadas
Implementación de controles	Hacer Seguimiento, monitoreo y actualización a los indicadores asociadas al Modelo de Seguridad y Privacidad de la Información.	Seguimiento a los indicadores de gestión.
	Realizar de manera anual un ejercicio de análisis de vulnerabilidades al interior de la entidad.	Informes de Ejecución de Análisis de vulnerabilidad externo
Gestión de incidentes	Implementar los lineamientos y actividades descritas en el procedimiento y la guía de gestión de incidentes de Seguridad de la Información	Informe de incidentes eventos e incidentes reportados al MINTIC.

 <p>ALCALDIA DE BUARAMANGA</p> <p>Caja de Previsión Social Municipal</p>	PROCESO DE GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN		Código: GTI-P003	
	PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN		Versión: 0	Pág. 10 11
			Fecha Aprobación: 30/01/2025	

CONTROL DE CAMBIOS DEL DOCUMENTO					
VERSIÓN	FECHA	DESCRIPCIÓN DE AJUSTES	ELABORÓ	REVISÓ	APROBÓ
0	30/01/2025	Emisión Inicial	Jhonatan Tique Marín Profesional Universitario Sistemas	Liliana M. Delgado C. Profesional de Calidad	APROBADO EN COMITÉ MIPG ACTA N° 005 de 2025 del 30/01/2025

COPIA CONTROLADA