PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

ALCALDIA DE BUCARAMANGA

Oficina Asesora TIC

2023

TABLA DE CONTENIDO

1. OBJETIVO

Establecer la estrategia de Seguridad y Privacidad de la Información para el periodo 2024-2025 del Municipio de Bucaramanga. El objetivo primordial del presente Plan Estratégico de Seguridad de la Información, en adelante PESI, es el de salvaguardar toda la información institucional mediante una gestión de riesgos eficaz y la implementación de controles adecuados. Esta iniciativa se orienta a preservar la confidencialidad, integridad y disponibilidad de los activos de información que respaldan los procesos institucionales, implementando así un entorno seguro y controlado contra posibles amenazas y vulnerabilidades.

2. OBJETIVOS ESPECÍFICOS

- Garantizar que la estrategia de Seguridad de la Información se encuentre alineada con las metas y objetos institucionales.
- Establecer y desarrollar las iniciativas y actividades para el cumplimiento efectivo de la estrategia de Seguridad de la Información.
- Definir las medidas técnicas, administrativas y relacionadas con el talento humano para la implementación y mejoramiento continuo del Modelo de Seguridad y Privacidad de la Información – MSPI.
- Planificar el seguimiento, medición y análisis de los controles implementados para la adopción del Modelo de Seguridad y Privacidad de la Información - MSPI.
- Asegurar el respaldo y compromiso de la Dirección a través del apoyo y fortalecimiento de las actividades y acciones encaminadas a la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

3. ALCANCE

Este plan se extiende a todos los procesos, al recurso humano y, en términos generales, a cada activo de información que respalda las diversas operaciones internas de la entidad.

Es fundamental subrayar que la aplicación efectiva de este plan se alinea directamente con el alcance delineado en la Política de Seguridad de la Información, así como con las pautas establecidas en el Documento Maestro del Modelo de Seguridad y Privacidad de la Información (MSPI) adoptados en la Alcaldía de Bucaramanga. Este enfoque estratégico garantiza que las medidas de seguridad implementadas sean coherentes con las directrices más amplias y las mejores prácticas definidas en los marcos normativos y estándares pertinentes.

4. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- **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)"
- **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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) 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
- **Resolución Municipal 0350 del 28 de noviembre de 2023 y Política de Tratamiento de Datos Personales del Municipio de Bucaramanga**

5. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Con el propósito de identificar el nivel de madurez frente a la implementación de los lineamientos y controles establecidos en el Modelo de Seguridad y Privacidad de la Información - MSPI, la Alcaldía de Bucaramanga desarrolló el autodiagnóstico correspondiente a la vigencia 2023 a través del *"Instrumento de Identificación de Linea Base de Seguridad de la Información"* herramienta proporcionada por el Ministerio de TIC. Este análisis contempla la totalidad de los procesos y activos de información que respaldan las diversas operaciones de la Entidad.

El objetivo fundamental de este autodiagnóstico consiste en evaluar de manera integral la eficacia de las medidas de seguridad existentes y detectar posibles áreas de mejora. Al involucrar todos los procesos y activos de información, garantizamos una evaluación integral que nos permita identificar y abordar de manera proactiva cualquier vulnerabilidad o riesgo potencial sobre los activos de información e infraestructura tecnológica.

5.1 Evaluación de Efectividad de controles – ISO 27001:2013 Anexo A

Este componente se encarga de medir el grado de implementación de los diferentes Dominios y sus objetivos de control definidos en el Anexo A de la Norma ISO 27001:2023. Dentro de los resultados obtenidos para este componente se puede evidenciar que la Alcaldía de Bucaramanga se encuentra en un nivel de implementación “Repetible” de acuerdo con los parámetros de evaluación establecidos en el Instrumento de Evaluación definido por el Ministerio de las TIC.

Frente al análisis realizado sobre este componente se puede evidenciar que los diferentes controles que se han implementado impactan positivamente los diferentes procesos, pero

se requiere de un mejoramiento continuo que permita lograr una formalización, comunicación y adopción adecuada sobre las buenas prácticas establecidas y procedimientos de seguridad de la información en toda la Entidad.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	32	100	REPETIBLE
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	34	100	REPETIBLE
A.8	GESTIÓN DE ACTIVOS	20	100	INICIAL
A.9	CONTROL DE ACCESO	38	100	REPETIBLE
A.10	CRIPTOGRAFÍA	10	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	33	100	REPETIBLE
A.12	SEGURIDAD DE LAS OPERACIONES	29	100	REPETIBLE
A.13	SEGURIDAD DE LAS COMUNICACIONES	42	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	40	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	20	100	INICIAL
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	46,5	100	EFECTIVO
PROMEDIO EVALUACIÓN DE CONTROLES		34	100	REPETIBLE

Figura 1. Evaluación de Efectividad de controles ISO 27001:2013 Anexo
Fuente: Tomado de "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" MinTIC.

Figura 2. Escala de Valoración de Controles vigencia 2023

Fuente: Elaboración Propia.

Figura 3. Brecha Anexo A ISO 27001 vigencia 2023
Fuente: Tomado de "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" MinTIC.

5.2 Avance del Ciclo de Funcionamiento del Modelo de Operación – PHVA

El Ciclo de Operación PHVA pretende determinar el nivel de gestión y formalización de los requisitos establecidos en el estándar ISO 27001:2013. Dentro del avance registrado para la Alcaldía de Bucaramanga se identificó que las diferentes fases del ciclo de funcionamiento del modelo de operación se encuentran en un nivel inicial y requiere continuar con la implementación de todos los requisitos normativos, legales y de seguridad definidos para el establecimiento e implementación del Modelo de Seguridad y Privacidad de la Información al interior de la Entidad.

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	17%	40%
	Implementación	4%	20%
	Evaluación de desempeño	4%	20%
	Mejora continua	4%	20%
TOTAL	TOTAL	29%	100%

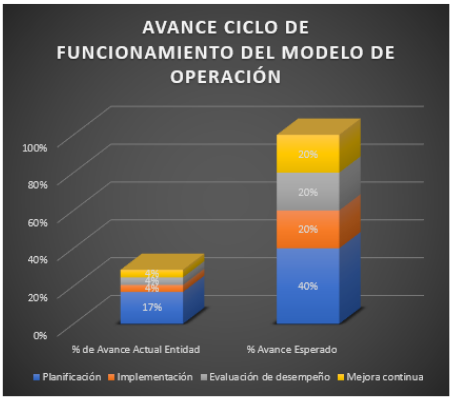

Figura 4. Avance de Implementación del ciclo PHVA vigencia 2023
Fuente: Tomado de "INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD" MinTIC.

5.3 Calificación frente a mejores prácticas en Ciberseguridad – NIST

Este componente tiene como objetivo central la evaluación de la implementación de buenas prácticas en ciberseguridad, siguiendo las directrices del marco de trabajo NIST. Este marco, diseñado para respaldar la identificación, detección, respuesta y recuperación, se orienta a fortalecer la gestión integral de riesgos de ciberseguridad al interior de la Entidad. Al alinearnos con el marco de trabajo NIST, buscamos no solo cumplir con estándares reconocidos a nivel internacional, sino también fortalecer nuestra capacidad para anticipar, mitigar y responder a amenazas cibernéticas.

La evaluación de las recomendaciones dentro de las 5 funciones del marco de trabajo NIST revela que los lineamientos asociados con la protección, respuesta y recuperación presentan un nivel de implementación considerablemente bajo. Este análisis subraya la necesidad imperativa de diseñar una estrategia de seguridad integral que aborde específicamente los riesgos relacionados con la ciberseguridad. El objetivo de esta estrategia es asegurar una respuesta efectiva y una recuperación oportuna en el caso de un escenario adverso que amenace la seguridad de la información. Esto implica no solo la implementación de medidas preventivas mejoradas, sino también la creación de protocolos

de respuesta claros y eficientes, así como la capacidad de recuperación para minimizar el impacto en caso de incidentes cibernéticos.

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
IDENTIFICAR	45	100
DETECTAR	41	100
RESPONDER	28	100
RECUPERAR	33	100
PROTEGER	33	100

Figura 5. Calificación Frente A Mejores Prácticas En Ciberseguridad (Nist)
Fuente: Tomado de “INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD” MinTIC.

6. ESTRATEGIA DE SEGURIDAD DIGITAL

La Alcaldía de Bucaramanga desarrollará una estrategia integral de seguridad de la información alineada con los estándares y buenas prácticas establecidas en el Modelo de Seguridad y Privacidad de la Información (MSPI). Esta iniciativa se materializará a través de la implementación de políticas, manuales, procedimientos, formatos y la adopción de mecanismos técnicos, administrativos y relacionados con el talento humano.

El propósito fundamental de esta estrategia es asegurar de manera efectiva la información, la infraestructura tecnológica y todos los activos de información de la Alcaldía de Bucaramanga. Se pondrá un énfasis especial en preservar la confidencialidad, integridad y disponibilidad de la información institucional.

Esta estrategia estará fundamentada en un enfoque proactivo de gestión de riesgos de seguridad de la información, acompañado de la implementación de controles efectivos para una mitigación adecuada. Se establecerán, además, estrategias específicas destinadas a la gestión oportuna y adecuada de incidentes de seguridad digital y el establecimiento de una cultura de seguridad de la información, orientada a fortalecer las habilidades de todos los usuarios y terceros dentro de la entidad. Además, se implementarán estrategias

específicas orientadas a la protección de la información de los ciudadanos, reafirmando nuestro compromiso de ofrecer servicios confiables y seguros a través de las Tecnologías de la Información y las Comunicaciones.

Esta iniciativa no solo busca cumplir con estándares de seguridad, sino también consolidar un entorno digital que promueva la confianza y la transparencia en todas nuestras operaciones. A través de esta estrategia, la Alcaldía de Bucaramanga se compromete a mantenerse a la vanguardia en la protección de la información y asegurando la continuidad de los servicios prestados.

En virtud de lo anterior, La Alcaldía de Bucaramanga define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

Figura 6. Estrategia de Seguridad de la Información
Fuente: Tomado de "PRODUCTO TIPO:
PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" MinTIC.

6.1. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021 expedida por el Ministerio de TIC:

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 Seguridad y Privacidad de la Información (MSPI) en nuestra entidad. 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.
Gestión de riesgos	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. 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. 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.
Concientización	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.
Implementación de controles	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. 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 perdida de información y/o la interrupción de los servicios tecnológicos que soportan los diferentes procesos al interior de la entidad.

Tabla 1. Estrategias específicas (ejes) Plan de Estratégico de Seguridad de la Información

7. DEFINICIÓN DE ACTIVIDADES ASOCIADAS AL PLAN ESTRATEGICO DE SEGURIDAD DE LA INFORMACIÓN

La Alcaldía de Bucaramanga define los siguientes proyectos y 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 seguridad de la información	1. 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).	1.1. Informe de Políticas definidas y aprobadas en el comité de gestión y desempeño MIPG y el CICCI.
	2. 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.	2.1. Implementación de proyectos asociados a Seguridad de la información y Ciberseguridad ejecutados al interior de la entidad.
Gestión de riesgos	3. Hacer Seguimiento, monitoreo y actualización al mapa de riesgos de seguridad de la información.	3.1. Inventario de activos de información actualizado.
	4. Hacer Seguimiento, monitoreo y actualización al inventario de activos de información.	4.1. Mapa de Riesgos de Seguridad de la Información actualizado.
	5. Diseño de una estrategia que permita hacer	5.1. Informe de seguimiento al Plan de Tratamiento

	seguimiento al Plan de tratamiento de riesgos de seguridad de la información de la entidad.	de Riesgos de Seguridad de la Información
Concientización	6. 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.	6.1. Plan de capacitación y Sensibilización.
		6.2. Informe con los resultados obtenidos durante los ejercicios y campañas realizadas
Implementación de controles	7. Diseñar una estrategia que permita a la entidad realizar un análisis externo de cumplimiento de los controles asociados a la norma ISO 27001.	7.1. Documento con estrategia para auditoría externa basada en ISO 27001.
	8. Realizar un ejercicio interno basado en el cumplimiento de los requisitos de la norma ISO 27001.	8.1. Informe de resultados auditoría interna basada en los requerimientos de la norma de ISO-27001
	9. Hacer Seguimiento, monitoreo y actualización a los indicadores asociadas al Modelo de Seguridad y Privacidad de la Información.	9.1. Seguimiento a los indicadores de gestión.
	10. Realizar de manera semestral un ejercicio de	10.1. Informes de Ejecución de Análisis de vulnerabilidad externo.

	análisis de vulnerabilidades al interior de la entidad.	
	11. Diseñar y ejecutar el plan de implementación de los controles para la remediación de las vulnerabilidades encontradas.	11.1. Informe de resultados de ejecución de plan de remediaciones de vulnerabilidades.
Gestión de incidentes	12. Implementar los lineamientos y actividades descritas en el procedimiento y la guía de gestión de incidentes de Seguridad de la Información	12.1. Informe de incidentes eventos e incidentes reportados al MINTIC.
	13. Realizar un ejercicio semestral que permita validar los tiempos de respuesta y acciones descritas en el procedimiento de gestión de incidentes de seguridad digital.	13.1. Bitácora de eventos y/o incidentes de seguridad de la información diligenciada de acuerdo con el procedimiento. 13.2. Informe semestral de resultados de ejercicio de validación del procedimiento de gestión de incidentes de seguridad digital.

Tabla 2. Actividades recomendadas para el Plan de Estratégico de Seguridad de la Información

8. CRONOGRAMA DE ACTIVIDADES / PROYECTOS:

Teniendo en cuenta los proyectos y actividades definidos en la sección anterior, se establece el siguiente cronograma con el propósito de definir los tiempos estimados para la realización de las actividades planteadas.

	MES											
ACTIVIDAD	01	02	03	04	05	06	07	08	09	10	11	12
Seguimiento, monitoreo y actualización a las políticas, manuales, procedimientos, guías, formatos, entre otros asociados a Modelo de Seguridad y Privacidad de la Información (MSPI).												
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.												
Seguimiento, monitoreo y actualización al mapa de riesgos de seguridad de la información.												
Seguimiento, monitoreo y actualización al inventario de activos de información.												
Diseño de una estrategia que permita hacer seguimiento al Plan de tratamiento de riesgos de seguridad de la información de la entidad.												
Implementar 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.												
Diseñar una estrategia que permita a la entidad realizar un análisis externo de cumplimiento de los controles asociados a la norma ISO 27001.												

Realizar un ejercicio interno basado en cumplimiento de los requisitos de la norma ISO 27001.												
Hacer Seguimiento, monitoreo y actualización a los indicadores asociadas al Modelo de Seguridad y Privacidad de la Información.												
Realizar de manera semestral un ejercicio de análisis de vulnerabilidades al interior de la entidad.												
Diseñar y ejecutar el plan de implementación de los controles para la remediación de las vulnerabilidades encontradas.												
Implementar los lineamientos y actividades descritas en el procedimiento y la guía de gestión de incidentes de Seguridad de la Información												
Realizar un ejercicio semestral que permita validar los tiempos de respuesta y acciones descritas en el procedimiento de gestión de incidentes de seguridad digital.												

Tabla 3. Cronograma propuesto para el Plan de Estratégico de Seguridad de la Información

9. ANÁLISIS PRESUPUESTAL

Con base en los proyectos definidos a continuación se mencionan aquellos ítems relacionados con seguridad de la información del cual se tiene conocimiento que se recomiendan sean incluidos como mínimo en los proyectos mencionados en la actividad 2, de igual forma se recomienda durante el primer semestre de 2024 realizar una revisión de este documento y de ser necesario ajustarlo de acuerdo con las proyecciones de la administración entrante.

ITEM	FUENTE DE FINANCIACION	VALOR
Acondicionamiento data center infraestructura física (aire acondicionado)	Recursos propios	$ 140,000,000.00

Elementos de seguridad infraestructura física (firewall)	Recursos propios	$ 147,000,000.00
Elementos de seguridad infraestructura lógica (certificados de navegación segura)	Recursos propios	$ 5,000,000.00
Licencias de antivirus	Recursos propios	$ 85,000,000.00
Recurso humano	Recursos propios	$ 120,000,000.00
TOTAL		**$ 497,000,000.00**

Tabla 4. Presupuesto base recomendado para el Plan de Estratégico de Seguridad de la Información

10. RESPONSABLES

- Alcalde: Aprobar los documentos de Alto Nivel.
- Comité Institucional de Gestión y Desempleo – MIPG, Comité Institucional de Coordinación de Control Interno - CICCI: Aprobar documentos asociados al Modelo de Seguridad y Privacidad de la Información.
- Responsable de Seguridad Digital / CIO / Asesor TIC Despacho Alcalde: Coordinar las actividades de implementación del MSPI

11. HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	FECHA
0.0	Original Documento desarrollado por el Proceso Gestión de TIC con el fin de establecer la primera versión del PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	Diciembre-12-2023