ALCALDÍA MAYOR
DE BOGOTÁ D.C.

BOGOTÁ

Dirección de Tecnologias y Sistemas de la Información

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI - 2025)

TABLA DE CONTENIDO

1. INTRODUCCION.

En Colombia, el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en cumplimiento de su rol como ente rector en materia de transformación digital del Estado, ha establecido la Política de Gobierno Digital. Esta política tiene como objetivo fundamental garantizar los principios de confidencialidad, integridad y disponibilidad de la información, promoviendo la generación de valor público mediante el uso estratégico de las tecnologías de la información y las comunicaciones (TIC).

A través de esta política, se definen los lineamientos que deben ser implementados por las entidades de la Administración Pública, en el marco del Modelo Integrado de Planeación y Gestión (MIPG), con el fin de fortalecer la relación Estado-Ciudadano y mejorar la prestación de servicios públicos de manera proactiva, confiable y articulada.

En concordancia con la normatividad vigente y en el marco de la transformación digital, la Secretaría Distrital de Seguridad, Convivencia y Justicia SDSCJ implementa el Modelo de Seguridad y Privacidad de la Información (MSPI), mediante el cual se definen directrices y parámetros orientados a maximizar la eficiencia operativa, fortalecer la gestión de riesgos y minimizar la exposición a amenazas asociadas al uso de las tecnologías de la información y las comunicaciones (TIC) en el desarrollo de sus funciones misionales.

En este contexto, la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI) por parte de las entidades busca fomentar una mayor transparencia en la gestión pública, promoviendo la incorporación de buenas prácticas en materia de seguridad de la información. Este enfoque constituye un pilar fundamental para la implementación del concepto de seguridad digital, fortaleciendo la confianza en el uso de las tecnologías y en la protección de los activos de información institucionales.

2. OBJETIVO.

Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) en la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de la Política de Gobierno Digital y la normatividad vigente en materia de seguridad de la información.

3. ALCANCE

El Modelo de Seguridad y Privacidad de la Información (MSPI) será aplicable a todos los procesos, sistemas de información, aplicaciones, plataformas tecnológicas, servicios, así como al personal vinculado a la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ), incluyendo funcionarios, contratistas y terceros que gestionen o tengan acceso a información sensible o datos personales. Esta aplicabilidad garantiza un enfoque integral en la protección de los activos de información institucionales.

4. FASE DE DIAGNOSTICO

Con el propósito de identificar el nivel de madurez en la gestión de la seguridad y privacidad de la información, se realizó actividades basadas en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) y la Norma Técnica Colombiana NTC/ISO/IEC 27001.

4.1. Estado Actual de la Entidad.

El diligenciamiento y recolección de evidencias del instrumento del Modelo de Seguridad y Privacidad de la Información (MSPI), permiten obtener una calificación ponderada por cada dominio evaluado. Esta calificación se deriva de los valores registrados frente a los objetivos de control, conforme a lo establecido en las hojas de cálculo de la herramienta, denominadas “ADMINISTRATIVAS” y “TÉCNICAS.

El resultado obtenido para la evaluación del estado para la vigencia 2024, refleja el estado actual de los controles implementados en la Entidad. Esta evaluación se realizó conforme a los lineamientos establecidos en la Norma Técnica Colombiana NTC/ISO/IEC 27001 en el Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MinTIC, aplicable a todas las entidades del orden nacional y territorial. Los resultados permiten identificar el nivel de madurez alcanzado en materia de seguridad de la información y constituyen una base para la mejora continua del sistema de gestión.

En la Evaluación de Efectividad de controles se obtuvieron los siguientes resultados:

Fuente: Herramienta-Instrumento de Evaluación MSPI-Portada

De acuerdo con el grafico la calificación promedio de evaluación de controles es de 89/100 puntos, que permite evidenciar que la Entidad se encuentra en estado Optimizado sobre las medidas de control establecidas de seguridad y privacidad de la información, lo que establece la ejecución de las buenas prácticas y mejora continua en los procedimientos internos.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	91	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	96	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	90	100	**GESTIONADO**
A.9	CONTROL DE ACCESO	88	100	**OPTIMIZADO**
A.10	CRIPTOGRAFÍA	80	100	**GESTIONADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	87	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	91	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	83	100	**GESTIONADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86	100	**OPTIMIZADO**
A.15	RELACIONES CON LOS PROVEEDORES	90	100	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	94	100	**OPTIMIZADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	80	100	**GESTIONADO**
A.18	CUMPLIMIENTO	85	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		**89**	**100**	**OPTIMIZADO**

Tabla 1. Efectividad Controles - ISO27001 – Vigencia 2024.

4.2. Identificación del nivel de madurez.

El nivel de madurez del Modelo de Seguridad y Privacidad de la Información (MSPI) para la Secretaría Distrital de Seguridad, Convivencia y Justicia, corresponde a un estado de cumplimiento como “Optimizado”, lo que evidencia un alto grado de consolidación en los controles establecidos. Este nivel implica el compromiso institucional con la continuidad operativa y el mejoramiento continuo de las actividades orientadas a la preservación y protección de la seguridad y privacidad de la información.

El estado de madurez de la Entidad se basa en la aplicación efectiva de controles técnicos y administrativos sobre los recursos y plataforma tecnológica, los procedimientos internos, las practicas sostenibles, el uso de guías y manuales establecidos, soportes documentales y la utilización eficiente y eficaz de los recursos tecnológicos para el apoyo a las funciones inherentes de la Entidad.

4.3. Levantamiento de información.

En el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad ha llevado a cabo un proceso estructurado de levantamiento de información, mediante el cual se recopilaron y analizaron datos relevantes para identificar y evaluar los riesgos asociados a la seguridad y privacidad de la información.

Este proceso incluyó la revisión de documentación institucional, el análisis de sistemas de información y otras consideraciones técnicas y administrativas, permitiendo obtener una comprensión integral del entorno actual de seguridad.

Como resultado, se identificaron escenarios de riesgo, brechas y oportunidades de mejora que servirán de base para el diseño e implementación de estrategias y medidas orientadas a garantizar la confidencialidad, integridad y disponibilidad de la información.

El levantamiento de información se realizó utilizando el instrumento de identificación de la línea base de seguridad incluido en la herramienta del MSPI, conforme a los lineamientos establecidos por el MinTIC.

5. FASE DE PLANEACIÓN.

En la fase de planeación del Modelo de Seguridad y Privacidad de la Información (MSPI), se identifican y describen las tareas, acciones y resultados esperados en materia de seguridad y privacidad de la información, diseñados específicamente para la Entidad.

Esta planeación debe estar alineada con los objetivos institucionales y contemplar la implementación de medidas específicas de protección, sustentadas en una metodología de gestión de riesgos que permita priorizar acciones y asignar recursos de manera eficiente.

La correcta ejecución de esta fase garantiza una base sólida para la implementación progresiva de controles, la mitigación de riesgos y el fortalecimiento del entorno de seguridad digital de la Entidad.

Esta planeación busca mejorar las condiciones de protección de la información en los procesos y áreas institucionales, asegurando su alineación con los objetivos estratégicos y el cumplimiento de la normatividad vigente.

El estado actual de la fase de planeación para la Secretaría Distrital de Seguridad, Convivencia y Justicia se relaciona a continuación:

Metas	Resultados	Enlace
Política de Seguridad y Privacidad de la Información	Actualmente, la Entidad cuenta con una Política de Seguridad y Privacidad de la Información aprobada y publicada, la cual fue formalizada mediante la Resolución 0025 del 29 de enero 2021, expedida por el Comité de Gestión Institucional. Esta política establece los lineamientos generales para la protección de la información institucional y constituye un marco de referencia para la implementación de controles y buenas prácticas en materia de seguridad y privacidad de la información.	PO-GT-1 - Política de Seguridad y Privacidad de la Información Res. 0025 de 2021
Manual de Seguridad y Privacidad de la Información	El Manual de Seguridad y Privacidad de la Información de la Entidad se encuentra alineado con los lineamientos establecidos en la Norma ISO/IEC 27001 y es objeto de revisión y actualización anual, en concordancia con las dinámicas institucionales y los cambios en el entorno tecnológico y normativo. Esta práctica garantiza la vigencia, pertinencia y efectividad de las directrices contenidas en el manual, fortaleciendo el sistema de gestión de seguridad de la información.	Manual de Seguridad y Privacidad de la Información 2025
Procedimientos	La Dirección de Tecnologías y Sistemas de la Información dispone de nueve procedimientos documentados, los cuales son revisados y actualizados periódicamente en función de las dinámicas del ejercicio institucional. Esta actualización continua permite asegurar la pertinencia, eficacia y alineación de dichos procedimientos con los objetivos estratégicos de la Entidad y con los lineamientos establecidos en materia de seguridad y privacidad de la información. ❖ PD-GT-1 Procedimiento de Gestión de Requerimientos de TI. ❖ PD-GT-2 Procedimiento de Gestión de Cambios. ❖ PD-GT-4 Procedimiento de Gestión de proyectos de TI ❖ PD-GT-6 Procedimiento Gestión de Incidentes o Problemas. ❖ PD-GT-8- Gestión y Administración de Usuarios. ❖ PD-GT-11 Gestión de Infraestructura y Plataformas Tecnológicas. ❖ PD-GT-13 Procedimiento De Uso Y Apropiación. ❖ PD-GT-17 Procedimiento Ciclo de vida de desarrollo de Software. ❖ PD-GT-18 Gestión De Datos Abiertos	Procedimientos DTSI

Roles y Responsabilidades	La Entidad cuenta con la publicación actualizada del formato F-GT-953 "Matriz de Roles y Responsabilidades de Seguridad de la Información", el cual ha sido diligenciado y se encuentra incorporado como anexo del Manual de Seguridad y Privacidad de la Información. Este documento permite establecer de manera clara las funciones, responsabilidades y niveles de autoridad relacionados con la gestión de la seguridad de la información, fortaleciendo la gobernanza y el cumplimiento de los lineamientos institucionales. La Matriz de roles y responsabilidades de Seguridad de la Información se encuentra publicada en el portal MIPG, de la Secretaría Distrital de Seguridad Convivencia y Justicia.	Matriz Roles y Responsabilidades
Inventario de activos de información.	La actualización del inventario de activos de información se realiza conforme a los lineamientos establecidos en la Política de Administración de Riesgos de la Entidad y en la Guía G-GD-01 - de Gestión de Activos de Información e Índice de Información Clasificada y Reservada. Esta actividad se lleva a cabo mediante el diligenciamiento del formato F-GD-1081 - Matriz de Registro de Activos de Información e Índice de Información Clasificada y Reservada, el cual permite mantener un control actualizado sobre los activos críticos, su clasificación y la valoración de criticidad de los activos, en concordancia con los principios de confidencialidad, integridad y disponibilidad.	Inventario Activos de Información
Integración del MSPI con el Sistema de Gestión documental	La Entidad alinea toda la documentación relacionada con la seguridad de la información —incluyendo políticas, procedimientos, planes, manuales, guías, instructivos y demás documentos— conforme a los lineamientos establecidos en materia de gestión documental institucional. Esta documentación es objeto de actualización periódica, en función de las dinámicas organizacionales y los requerimientos normativos o técnicos que surjan. Toda la información se encuentra disponible y accesible a través del Portal MIPG de la Secretaría, garantizando su consulta, trazabilidad y control.	Gestión Documental
Identificación, Valoración y tratamiento de riesgo.	La Entidad cuenta con la Matriz de Riesgos de Seguridad de la Información, elaborada conforme a los lineamientos establecidos en la Política de Administración de Riesgos Institucional. Esta herramienta permite identificar, analizar, valorar y tratar los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, asegurando una gestión proactiva y alineada con los objetivos estratégicos y normativos de la Entidad. El seguimiento a los riesgos de seguridad de la información se realiza de forma cuatrimestral, de acuerdo con las consideraciones establecidas en la Guía de Administración de Riesgos de la Entidad.	Matriz de Riesgos de Seguridad de la Información Informe de Riesgos de Seguridad de Información
Plan de Comunicaciones.	La Dirección de Tecnologías y Sistemas de la Información cuenta con un Plan de Uso y Apropiación orientado a fortalecer la cultura organizacional en materia de seguridad y privacidad de la información. Este plan contempla diversas actividades de sensibilización y divulgación, desarrolladas a través de canales institucionales como el correo electrónico, la intranet, boletines informativos y presentaciones internas. Entre las acciones implementadas se destacan: ❖ Diseño y difusión de piezas gráficas con recomendaciones sobre seguridad digital, abordando temas como spam, phishing, malware, ransomware e ingeniería social, así como contenidos relacionados con la Política y el Manual de Seguridad y Privacidad de la Información. ❖ Charlas e inducciones dirigidas a funcionarios y contratistas, enfocadas en el Sistema de Gestión de Seguridad de la Información (SGSI), el Procedimiento de Gestión de Incidentes y la Protección de Datos Personales. ❖ Divulgación de documentación oficial relacionada con el SGSI, con el fin de promover su conocimiento, aplicación y cumplimiento en todos los niveles de la Entidad.	GT-UA-2025-V1-Plan de Uso y Apropiación.xlsx

Tabla 2. Metas y Resultados Fase de Planeación.

6. FASE DE IMPLEMENTACIÓN.

En la fase de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad planea, ejecuta y supervisa las actividades necesarias para dar cumplimiento a los requisitos establecidos en materia de seguridad y privacidad de la información.

Estas acciones se desarrollan en el marco de los diferentes planes institucionales y están alineadas con la normatividad interna y externa vigente, lo que permite establecer un entorno de control robusto que garantiza la confidencialidad, integridad y disponibilidad de la información.

La implementación efectiva de esta fase fortalece la capacidad institucional para prevenir, detectar y responder a incidentes de seguridad, asegurando la continuidad operativa y el cumplimiento de los objetivos estratégicos.

El estado actual de la fase de implementación para la Secretaría Distrital de Seguridad, Convivencia y Justicia se relaciona a continuación:

Metas	Resultados	Enlace
Plan de Seguridad y Privacidad de la Información	La Entidad ha diseñado y estructurado el Plan de Seguridad y Privacidad de la Información, en el cual se definen las actividades a desarrollar durante cada vigencia, con el objetivo de fortalecer las condiciones de seguridad en los distintos procesos de la Secretaría. Este plan tiene una periodicidad anual y está orientado al cumplimiento de las metas establecidas, en concordancia con los principios de mejora continua, gestión del riesgo y alineación con los objetivos institucionales.	Plan de Seguridad y Privacidad de la Información
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	La Entidad ha diseñado y estructurado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, en el cual se establecen las actividades necesarias para realizar el seguimiento a los controles de riesgos en cada vigencia. Este seguimiento tiene como objetivo fortalecer las condiciones de seguridad en los distintos procesos de la Secretaría. El plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información tiene una periodicidad anual, lo que permite evaluar y cumplir las metas establecidas de manera continua y sistemática.	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Gestión de Cambios	A través del procedimiento PD-GT-02 Gestión de Cambios, se definen las actividades necesarias para la gestión y actualización de las soluciones tecnológicas de la Entidad. Cada cambio propuesto debe ser presentado en una reunión Gestión de Cambios, donde se validan y aprueban los parámetros establecidos en la documentación correspondiente. La gestión y documentación de los cambios se realiza mediante la Consola de Mesa de Servicios, habilitada específicamente para este propósito. Toda la información generada es actualizada y almacenada en los repositorios designados, garantizando su disponibilidad para consulta. Es importante destacar que toda gestión de cambios debe ser aprobada por el grupo de gestión de cambios, conforme a lo estipulado en el procedimiento mencionado.	PD-GT-2 Procedimiento gestión de Cambios.
Indicadores	La Entidad diseña y establece indicadores de desempeño e indicadores de gestión, con el propósito de validar la información relacionada con los procedimientos institucionales en materia de seguridad de la información. Estos indicadores permiten evaluar el cumplimiento, la eficacia y la mejora continua de los procesos establecidos, asegurando una gestión alineada con los objetivos estratégicos de la Entidad.	Indicadores
Transición IPV4 a IPV6	el cumplimiento a satisfacción del protocolo IPV6 en la Secretaría Distrital de Seguridad, Convivencia y Justicia, después de la revisión del	IPV4 a IPV6

	funcionamiento de la soluciones y servicios tecnológicos que fueron objeto de la adopción del protocolo IPV6 durante la fase de implementación en cumplimiento a la resolución 2710 de 2017 y la resolución 1126 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones.	

Tabla 3. Metas y Resultados Fase de Implementación.

7. FASE DE EVALUACIÓN DE DESEMPEÑO.

En la fase de evaluación del desempeño del Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad analiza y revisa la efectividad de las medidas implementadas para proteger la información, lo que implica la recopilación y el análisis de datos sobre auditorías internas y externas, y revisiones periódicas de cumplimiento.

La característica principal es identificar fortalezas y debilidades en el sistema de seguridad, así como medir la eficiencia y efectividad de los controles establecidos. Los resultados obtenidos en esta fase permiten a la Entidad tomar decisiones informadas para ajustar y mejorar las políticas y procedimientos de seguridad y privacidad, garantizando una protección continua y eficaz de la información.

El estado actual de la fase de Evaluación de Desempeño para la Secretaría Distrital de Seguridad, Convivencia y Justicia se relaciona a continuación:

Metas	Resultados	Enlace
Herramienta - MSPI	Se realiza actualización y recopilación de evidencias del instrumento evaluación del Modelo de Seguridad y Privacidad de la información – MSPI, donde se recopilan los datos de la efectividad de controles – ISO 27001, con las evidencias documentales de los procedimientos y/o los enlaces de referencia de consulta, se realiza actualización de la hoja de levantamiento de información del instrumento evaluación MSPI. Se anexa carpeta de evidencias de documentación recopilado y documento Instrumento evaluación MSPI. El Modelo de Seguridad y Privacidad de la Información (MSPI) vigente, se encuentra publicado en los repositorios SharePoint para la Dirección de Tecnología.	Instrumento de Autodiagnóstico de Seguridad y Privacidad de la Información.xlsx
Plan de Ejecución de Auditorias	La Entidad cuenta con un Plan Anual de Auditoría para cada vigencia, mediante el cual se evalúa la eficacia y eficiencia del Sistema de Control Interno. Este plan contempla auditorías y seguimientos independientes, diseñados para agregar valor y contribuir al mejoramiento continuo de los procesos institucionales. Las auditorías se desarrollan bajo un enfoque sistemático, basado en la gestión de riesgos y en procesos de aseguramiento, alineados con el cumplimiento de los objetivos estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia.	Plan Anual de Auditoria

Tabla 4. Metas y Resultados Fase de Evaluación y Desempeño.

8. FASE DE MEJORA CONTINUA

En la fase de mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad se enfoca en implementar y ajustar acciones basadas en los resultados de las evaluaciones de desempeño anteriores. El objetivo es fortalecer de manera progresiva los controles y procesos de seguridad, permitiendo una adaptación efectiva frente a nuevas amenazas y a los cambios en las necesidades organizacionales.

Durante esta fase, se analizan las áreas de mejora identificadas y se desarrollan planes específicos para abordar las debilidades detectadas. Esto puede incluir la actualización de

políticas, la implementación de nuevas tecnologías de seguridad, y la capacitación adicional del personal.

La Entidad también establece métricas y realiza un seguimiento constante de los cambios implementados para asegurarse de que estos produzcan los resultados deseados. La documentación detallada de estos procesos y sus resultados es crucial para permitir la transparencia y la responsabilidad en la gestión de la seguridad y privacidad de la información.

El estado actual de la fase de Evaluación de Desempeño para la Secretaría Distrital de Seguridad, Convivencia y Justicia se relaciona a continuación:

Meta	Resultado	Enlace
Planes de Mejoramiento	Plan de Mejoramiento Externo.	Planes de Mejoramiento
	Plan de Mejoramiento Interno.	

Tabla 5. Metas y Resultados Fase Mejora Continua.

9. CONCLUSIONES

- El Modelo de Seguridad y Privacidad de la Información (MSPI) permite a la Entidad cumplir con las normativas y estándares nacionales e internacionales en materia de seguridad y privacidad de la información. Este modelo proporciona un marco estructurado que garantiza la protección de los activos de información, alineando las prácticas institucionales con los requisitos legales y las mejores prácticas reconocidas a nivel global.

- La implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) promueve una cultura organizacional orientada a la mejora continua. A través de evaluaciones periódicas y la incorporación de lecciones aprendidas, la Entidad puede adaptarse de manera proactiva a nuevas amenazas y desafíos, manteniendo una postura de seguridad sólida y resiliente en el tiempo.

- Gracias al Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad puede identificar, evaluar y mitigar de manera eficaz los riesgos asociados a la seguridad y privacidad de la información. Esta capacidad reduce significativamente la probabilidad de ocurrencia de incidentes de seguridad y minimiza su impacto potencial, fortaleciendo así la resiliencia institucional frente a amenazas emergentes.

- El Modelo de Seguridad y Privacidad de la Información (MSPI) establece condiciones óptimas para garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo así los activos de información más valiosos de la Entidad. Este enfoque integral asegura que los datos estén resguardados contra accesos no autorizados, modificaciones indebidas y pérdidas, fortaleciendo la confianza en los sistemas institucionales.