MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI)

2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCION.

Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en aras de garantizar los principios de Integridad, confidencialidad y disponibilidad de la información, establece la Política de Gobierno Digital, la cual genera los lineamientos a ejecutar y/o aplicar por las entidades de la Administración Pública.

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC juega un papel crucial en la definición de estándares y políticas para asegurar que todas las entidades gubernamentales adopten prácticas sólidas de gestión de seguridad de la información."

En observancia a la Política de Gobierno Digital, las entidades estatales desarrollan estrategias de gestión que facilitan su óptimo funcionamiento y el cumplimiento de la misión institucional y la continuidad del negocio.

En ese orden de ideas, la Secretaría Distrital de Seguridad, Convivencia y Justicia SDSCJ adoptó la Política de Seguridad y Privacidad de la Información de acuerdo con la normatividad vigente, la Entidad debe implementar el Modelo de Seguridad y Privacidad de la Información – MSPI estableciendo directrices y parámetros en el marco de la transformación digital que permitan maximizar la efectividad de los procesos y minimizar la exposición y ejecución de riesgos derivados del uso de las tecnologías de la información y las comunicaciones, en el diario trasegar de Entidad.

Para lo cual, mediante la adopción Modelo de Seguridad y Privacidad por parte de las Entidad, se busca fomentar un aumento en la transparencia de la Gestión Pública, impulsando la adopción de las mejores prácticas en Seguridad de la Información como fundamento para la implementación del concepto de Seguridad Digital

2. OBJETIVO.

Implementar el Modelo de Seguridad y Privacidad de la Información (MSPI) en la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ) para asegurar la integridad, confidencialidad y disponibilidad de la información, en conformidad con la Política de Gobierno Digital y la normatividad vigente. Esto incluirá la aplicación de las mejores prácticas y estándares internacionales, como ISO 27001.

3. ALCANCE

El MSPI será aplicable a todos los procesos, sistemas, aplicaciones, plataforma tecnológica, servicios y personal de funcionarios y contratistas de la SDSCJ que manejen o gestionen información sensible y datos personales, así como a los terceros que presten servicios a la Entidad.

4. DIAGNOSTICO

4.1. Estado Actual de la Entidad.

El diligenciamiento y recolección de evidencias del instrumento Modelo de Seguridad y Privacidad de la Información (MSPI), permite obtener una calificación ponderada para cada dominio a partir de los valores registrados sobre los objetivos de control de acuerdo con los establecido en las hojas de cálculo de la herramienta denominada como “ADMINISTRATIVAS” y “TECNICAS”.

El resultado obtenido para la evaluación del estado actual para la vigencia 2023, con sus respectivas evidencias, refleja el estado actual de los controles implementados en la Entidad de acuerdo con la normatividad establecida en la Norma Técnica Colombiana NTC/ISO/IEC 27001:2013 y lo planteado dentro del desarrollo del Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por MinTIC, para todas las entidades de orden nacional y territorial.

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 87/100 puntos, que permite evidenciar que la Entidad se encuentra en estado Optimizado sobre las medidas de control establecidas de seguridad y privacidad de

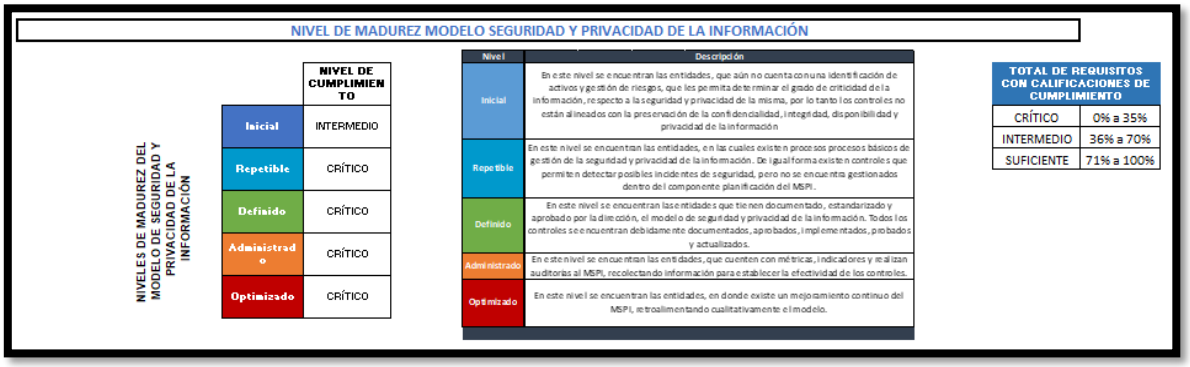
la información, lo que establece la ejecución de las buenas prácticas y mejora continua en los procedimientos internos.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	87	100	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	96	100	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	88	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	89	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	80	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		**87**	**100**	OPTIMIZADO

Tabla 1. Efectividad Controles - ISO27001:2013 – Vigencia 2023.

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, se encuentra en un nivel de cumplimiento como “Optimizado”, el cual establece como imperativo la continuidad y mejoramiento continuo de las actividades desarrolladas para la preservación y conservación de la seguridad y privacidad de la información.



El estado de madurez de la Entidad se basa en la recolección de evidencias de la aplicación efectiva de controles técnicos y administrativos sobre los recursos y

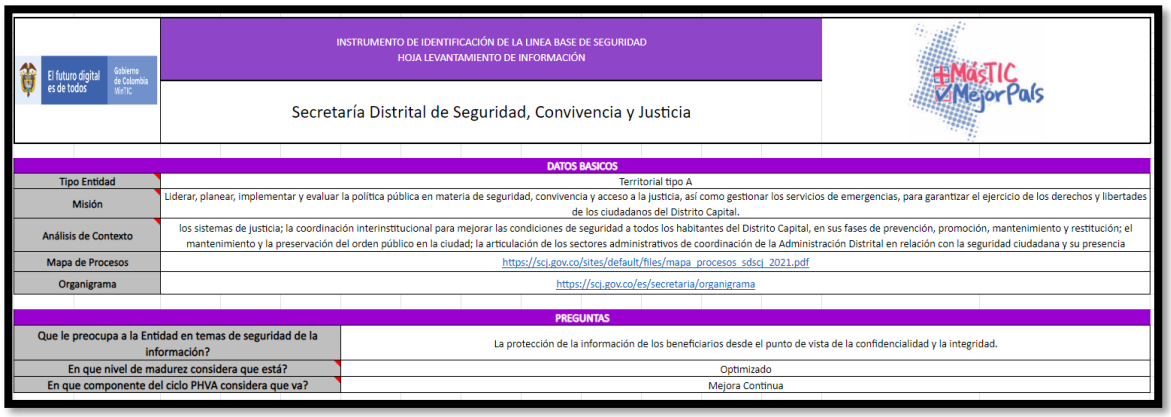
plataforma tecnológica, los procedimientos internos, las practicas sostenibles, el uso de guías y manuales establecidos, soportes documentales y la utilización eficiente y eficaz de los recursos tecnológicos para el apoyo a las funciones inherentes de la Entidad.

4.3. LEVANTAMIENTO DE INFORMACIÓN.

En el Levantamiento de Información del Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad ha recopilado y analizado datos relevantes para identificar y evaluar los riesgos de seguridad y privacidad de la información. Mediante revisiones de documentos y análisis de sistemas y demás consideraciones, obteniendo una comprensión amplia del entorno de seguridad actual, identificando posibles escenarios y oportunidades de mejoras para la seguridad de la información.

La información recopilada ahora sirve como base para desarrollar estrategias y medidas efectivas que protejan la información, garantizando su confidencialidad, integridad y disponibilidad.

El levantamiento de información se realizó mediante el instrumento de identificación de la línea base de seguridad de la herramienta del modelo de Seguridad y Privacidad de la información para tal fin.



INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

Secretaría Distrital de Seguridad, Convivencia y Justicia

DATOS BASICOS	
Tipo Entidad	Territorial tipo A
Misión	Liderar, planear, implementar y evaluar la política pública en materia de seguridad, convivencia y acceso a la justicia, así como gestionar los servicios de emergencias, para garantizar el ejercicio de los derechos y libertades de los ciudadanos del Distrito Capital.
Análisis de Contexto	los sistemas de justicia; la coordinación interinstitucional para mejorar las condiciones de seguridad a todos los habitantes del Distrito Capital, en sus fases de prevención, promoción, mantenimiento y restitución; el mantenimiento y la preservación del orden público en la ciudad; la articulación de los sectores administrativos de coordinación de la Administración Distrital en relación con la seguridad ciudadana y su presencia
Mapa de Procesos	https://scj.gov.co/sites/default/files/mapa_procesos_sdscj_2021.pdf
Organigrama	https://scj.gov.co/es/secretaria/organigrama

PREGUNTAS	
Que le preocupa a la Entidad en temas de seguridad de la información?	La protección de la información de los beneficiarios desde el punto de vista de la confidencialidad y la integridad.
En que nivel de madurez considera que está?	Optimizado
En que componente del ciclo PHVA considera que va?	Mejora Continua

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 de seguridad privacidad de la información diseñado para la Entidad. Esta planeación debe estar en concordancia con los objetivos institucionales y contemplar medidas específicas de seguridad y privacidad de la información, utilizando una metodología de gestión de riesgos.

La Entidad, en esta fase, determina el alcance del Modelo de Gestión de Seguridad de la Información (SGSI), estableciendo los parámetros y medidas de seguridad y privacidad para mejorar las condiciones de seguridad al interior de los procesos y áreas de esta.

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	En la actualidad se encuentra aprobado y publicado la política de seguridad y privacidad de la información para la Entidad la cual fue aprobada por el comité de Gestión Institucional, mediante resolución 0851 de 2019.	Política de Seguridad y Privacidad de la Información Resolución 0851 de 2019
Manual de Seguridad y Privacidad de la Información	El Manual de Seguridad y Privacidad de la Información, se encuentra alineado con la Norma ISO 27001.2013 y es actualizado de acuerdo con las dinámicas institucionales.	Manual de Seguridad y Privacidad de la Información
Procedimientos	La Entidad cuenta con 9 procedimientos que son actualizados de acuerdo con las dinámicas del ejercicio institucional. • 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	Se cuenta con la publicación de la versión actualizada del formato F-GT-953 “Matriz de roles y responsabilidades de Seguridad de la Información”, diligenciado como anexo del Manual de Seguridad y privacidad de la Información. 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 de activos de información se realiza de acuerdo con los parámetros establecidos en la Política de Administración de riesgos de la Entidad y la G-GD-01_V1_Guía De Gestión De Activos De Información E índice De Información Clasificada Y Reservada, a través del formato F-GD-1081 - Matriz Registro De Activos De Información E Índice De Información Clasificada Y Reservada. Las políticas y procedimientos se revisan y actualizan anualmente para adaptarse a las nuevas amenazas y cambios en la normativa.	Inventario Activos de Información
Integración del MSPI con el Sistema de Gestión documental	La Entidad alinea la documentación relacionada con seguridad de la información (políticas, procedimientos, planes, manuales, guías, instructivos y demás documentos) de acuerdo los parámetros establecidos sobre gestión documental, realizando actualización periódica de acuerdo con a las dinámicas y requerimientos que se requieran, la documentación se encuentra disponible en el Portal MIPG de la Secretaría.	Gestión Documental
Identificación, Valoración y tratamiento de riesgo.	La Entidad cuenta con la Matriz de Riesgos de Seguridad de la Información se realiza de acuerdo con los parámetros establecidos en la Política de Administración de riesgos de la Entidad.	Matriz de Riesgos de Seguridad de la Información
Plan de Comunicaciones.	Se cuenta con un plan de Uso y Apropiación al interior de la Dirección de Tecnologías y Sistemas de la Información donde se establecen las actividades descritas en el plan de uso y apropiación desplegadas a través de correo electrónico, intranet, boletines, presentaciones así: • Piezas Graficas sobre tips de seguridad: (Spam, Phishing, Malware, Ransomware, Ingeniería Social) y temas de seguridad: (Política de seguridad y Privacidad de la Información Manual de Seguridad y Privacidad de la Información.)	

	• Charlas e Inducción a funcionarios y/o contratistas sobre Sistema de Gestión de seguridad de la información SGSI, Procedimiento de Gestión de Incidentes, Protección de Datos Personales • Divulgación de documentación relacionada con el Sistema de Gestión de Seguridad de la Información.	

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 cumplir con los requisitos de seguridad y privacidad de la información, lo cual permite llevar a cabo las acciones establecidas en los diferentes planes, estas acciones están alineadas con las normatividad interna y externa, estableciendo un marco robusto para la integridad, disponibilidad y confidencialidad de la información.

Todas las actividades deben ser documentadas adecuadamente para evidenciar la ejecución, los resultados, y cualquier ajuste o actualización que mejore las condiciones de seguridad y privacidad de la información en la SDSCJ.

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 diseño y estructuro el plan de Seguridad y Privacidad de la Información donde se establecen las actividades a desarrollar en cada vigencia para el mejoramiento de las condiciones de seguridad en cada uno de los procesos de La Secretaría, la periodicidad de este plan es de forma anual para el cumplimento de las metas establecidas.	Plan de Seguridad y Privacidad de la Información
Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información	La Entidad diseño y estructuro el plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información donde se establecen las actividades para desarrollar el seguimiento a los controles de riesgos cada vigencia que permita el mejoramiento de las condiciones de seguridad en cada uno de los procesos de La Secretaría, la periodicidad de este plan es de forma anual para el cumplimento de las metas establecidas.	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
Gestión de Cambios	Mediante el proceso PD-GT-02 Gestión de Cambios se establecen las actividades propias para realizar la gestión y actualización de las soluciones tecnológicas de la Entidad, cada cambio debe pasar por reunión de gestión de cambios para la validación y aprobación de los parámetros descritos en los documentos establecidos, la documentación y gestión se realiza a través de la Consola de mesa de servicios dispuesta para tal fin. La documentación es actualizada y conservada en los repositorios que se determinaron para la consulta. Toda gestión de Cambios debe ser aprobada por el grupo de gestión de cambios que se establece de acuerdo con lo establecido en el procedimiento.	PD-GT-2 Procedimiento gestión de Cambios.
Indicadores	La Entidad diseña y establece Indicadores de desempeño e indicadores de gestión donde se realiza la validación de información referente a los procedimientos establecidos para la Entidad, referente a seguridad de la Información.	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 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.	IPV4 a IPV6

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 a través de auditorías internas y externas, utilizando metodologías como ISO 19011 para auditorías de sistemas de gestión.

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 continuamente las políticas y procedimientos de seguridad y privacidad, asegurando 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 vigencia 2022, donde se recopilan los datos de la efectividad de controles –ISO 27001:2013, 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.	
Plan de Ejecución de Auditorias	La Entidad cuenta con el plan anual de auditoria para todas las vigencias, donde se evalúa la eficacia y eficiencia del Sistema de Control Interno, a partir de auditorías y seguimientos independientes concebidos para agregar valor y mejorar los procesos de la Entidad, a través de un enfoque sistemático basado en riesgos y procesos de aseguramiento alineados al 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 mejorar continuamente los controles y procesos de seguridad para adaptarse a nuevas amenazas y cambiar las necesidades de la organización.

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 mejora continua 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.	
	Planes de Mejoramiento Rendición de Cuentas	

Tabla 5. Metas y Resultados Fase Mejora Continua.

9. CONCLUSIONES

- El Modelo de Seguridad y Privacidad de la Información (MSPI) permite que la Entidad cumpla con las normativas y estándares nacionales e internacionales de seguridad y privacidad de la información, como la ISO/IEC 27001.

- La implementación del MSPI fomenta una cultura de mejora continua. A través de evaluaciones periódicas y la incorporación de lecciones aprendidas, la Entidad puede adaptarse proactivamente a nuevas amenazas y desafíos, manteniendo siempre una postura de seguridad robusta.

- Gracias al Modelo de Seguridad y Privacidad de la Información (MSPI), la Entidad puede identificar, evaluar y mitigar eficazmente los riesgos de seguridad y privacidad de la información, asegurando la confidencialidad, integridad y disponibilidad de los datos.

- El MSPI establece condiciones óptimas de confidencialidad, integridad y disponibilidad de la información, protegiendo los activos de información más valiosos de la Entidad.