Control de cambios

Versión	Fecha	Descripción de la modificación
01	13 de febrero de 2020	Se aprueba el Plan de Seguridad y Privacidad de la Información de la Secretaría Distrital de Gobierno.
02	13 de febrero del 2021	Se ajusta las metas para la vigencia 2021
03	25 de mayo del 2021	Se ajusta el plan de seguridad de la información, de acuerdo con los siguientes ítems: ➢ Se actualiza los resultados del instrumento de Mintic vigencia 2021 ➢ Se actualiza cronograma de actividades vigencia 2021 ➢ Se ajusta la introducción ➢ Se adiciona capítulo del plan de trabajo, de acuerdo con la fase de implementación del MSPI
04	31 de enero 2022	Se realiza la actualización del plan de seguridad de para la vigencia 2022
05	30 de noviembre 2022	Se realiza la actualización del plan de seguridad de para la vigencia 2023
06	30 de enero de 2024	Se realiza la actualización del Plan de seguridad y Privacidad de la Información de para la vigencia 2024
07	28 de enero de 2025	Se realiza la actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2025
08	Xx de enero de 2026	Se realiza la actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2026

Método de Elaboración	Revisa	Aprueba
El documento se actualiza de acuerdo con las indicaciones de la Oficina Asesora de Planeación y los profesionales de la Dirección de Tecnologías e Información: Carlos Javier Díaz Rodríguez , Leonardo Sisrra Rodríguez y la auxiliar administrativa Doris Páez Romero.	**Mario Alexander Ortiz Salgado** Proceso Gerencia de TIC Director de Tecnologías e Información **Olga Milena Arias Aguirre** Promotora de Mejora **Leidy Johana Avila Arias** Revisión Metodológica - Profesional de la Oficina Asesora de Planeación **Angela Patricia Cabeza Morales** Revisión Plantilla Documental – Profesional de la Oficina Asesora de Planeación	**Carine Pening Gaviria** Líder del Macroproceso Gerencia de la Información Subsecretaría de Gestión Institucional El documento fue aprobado en sesión del Comité Institucional de Gestión y Desempeño-CIGD del xxx de xxxx de 2026 y publicado mediante Caso HOLA No. xxx

1. INFORMACIÓN GENERAL

Objetivo del Plan

Implementar y gestionar el Modelo de Seguridad y Privacidad de la Información - MPSI, con el objetivo de garantizar la confiabilidad, disponibilidad e integridad de los activos de información de la Secretaría Distrital de Gobierno de Bogotá, de acuerdo con los lineamientos de MINTIC - Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, el Departamento Administrativo de Función Pública y la Oficina Consejería Distrital TIC, en cumplimiento del marco normativo vigente y la Política Nacional de Seguridad Digital (CONPES 3995)

Responsable

Director(a) de Tecnologías e Información.
Oficial de Seguridad de la Información.

Glosario[1]

Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Confidencialidad: Propiedad de la información que se mantiene inaccesible y no se revela a individuos, entidades o procesos no autorizados.

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad autorizada.

Integridad: Propiedad de exactitud y completitud de la información.

No repudio: El no repudio en el envío de información a través de las redes es la capacidad de demostrar la identidad del emisor en el envío de la información a través de una red. Tiene como objetivo certificar que la información o datos provengan realmente de la fuente que dice ser.

Siglas

- **CIGD:** Comité Institucional de Gestión y Desempeño.
- **ColCERT:** Grupo de Respuestas a Emergencias Cibernéticas en Colombia.
- **CSIRT:** Computer Security Incident Response Team, Equipo de Respuesta ante Incidencias de Seguridad Informáticas.
- **DTI:** Dirección de Tecnologías e Información.
- **ISO**: Organización Internacional de Estandarización.

[1] Diciembre 2018. Consultoría "Guardianes de la Información". Alta Consejería Distrital de las Tics. http://ticbogota.gov.co/documentos/guardianes-la-informaci%C3%B3n

- **MINTIC**: Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.
- **MIPG:** Modelo Integrado de Planeación y Gestión.
- **MSPI:** Modelo de Seguridad y Privacidad de la Información.
- **PETI:** Plan Estratégico de Tecnologías e Información.
- **PHVA:** Planear, Hacer, Verificar, Actuar.
- **SIC:** Superintendencia de Industria y Comercio.
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **TIC:** Tecnologías de la Información y las Comunicaciones.

2. ESTRUCTURA DEL PLAN

2.1 Introducción

La Secretaría Distrital de Gobierno mediante Resolución 783 de 2018, modificada por la Resolución 236 de 2019 creo el Comité Institucional de Gestión y Desempeño como órgano rector y articulador de las acciones y estrategias que se desarrollen para la correcta implementación, operación, seguimiento y fortalecimiento del Modelo Integrado de Planeación y Gestión MIPG, como marco de referencia del Sistema de Gestión Institucional.

Esta resolución, estableció las responsabilidades para cada una de las dimensiones y políticas de MIPG en la cual la Subsecretaría de Gestión Institucional quedó a cargo de las Políticas de Gobierno Digital y Seguridad Digital de la dimensión de Gestión con Valores para Resultados. De acuerdo con esta responsabilidad, la Dirección de Tecnologías e Información, es quien define la Política de Seguridad, Privacidad de la Información y Seguridad Digital, la cual se encuentra establecida en el Manual de Gestión de Seguridad de la Información GDI-TIC-M004.

Igualmente se tienen en cuenta las directrices establecidas en las buenas prácticas de la norma ISO/IEC 27001:2013, ISO/IEC 27001:2022 ISO/IEC 27002:2013, ISO/IEC 27002:2022 así como los lineamientos que emite el Ministerio de Tecnologías de la Información y las Comunicaciones, garantizando la evolución y permanencia de su implementación y el marco normativo de la Política Nacional de Seguridad Digital (CONPES 3995).

La implementación de este plan ayudará a identificar las responsabilidades en materia de seguridad y privacidad de la información, así como el desarrollo de las actividades necesarias para la identificación y clasificación de los activos de información con el fin de aplicar los controles de confidencialidad, integridad y disponibilidad bajo un entorno de mejora continua dentro del ciclo PHVA.

En cuanto al estado actual de los controles establecidos en la norma ISO/IEC 27001:2022 (Anexo A) actualizados por el MINTIC mediante la resolución 2777 del 5 de junio del 2025, la Secretaría Distrital de Gobierno, viene realizando el proceso de identificación, actualización e incorporación en la evaluación de los controles con el instrumento en su nueva versión de autodiagnóstico del Min-Tic . Adicionalmente, se permiten evidenciar el seguimiento para las vigencias 2024, y 2025:

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

Evaluación de Efectividad de controles			
DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	90	100	OPTIMIZADO
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	71	100	GESTIONADO
SEGURIDAD DE LOS RECURSOS HUMANOS	69	100	GESTIONADO
GESTIÓN DE ACTIVOS	58	100	EFECTIVO
CONTROL DE ACCESO	51	100	EFECTIVO
CRIPTOGRAFÍA	40	100	REPETIBLE
SEGURIDAD FÍSICA Y DEL ENTORNO	39	100	REPETIBLE
SEGURIDAD DE LAS OPERACIONES	36	100	REPETIBLE
SEGURIDAD DE LAS COMUNICACIONES	53	100	EFECTIVO
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26	100	REPETIBLE
RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	51	100	EFECTIVO
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
CUMPLIMIENTO	32,5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES	50	100	EFECTIVO

Ilustración 1 Autodiagnóstico 2024

Para el autodiagnóstico con corte a diciembre de 2024, se ve reflejado un avance 50% de efectividad en la evaluación de los controles. Sin embargo, llegar al 100% de la calificación objetivo es difícil, debido a que no se puede contar con un Oficial de Seguridad o su equipo dentro de la planta de la entidad y plantea un plan de trabajo a corto y mediano plazo, que implica el compromiso de las directivas.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	79	100	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	69	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	64	100	GESTIONADO
A.9	CONTROL DE ACCESO	51	100	EFECTIVO
A.10	CRIPTOGRAFÍA	40	100	REPETIBLE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	43	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	44	100	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	53	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	26	100	REPETIBLE
A.15	RELACIONES CON LOS PROVEEDORES	50	100	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	49	100	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	30	100	REPETIBLE
A.18	CUMPLIMIENTO	32.5	100	REPETIBLE
PROMEDIO EVALUACIÓN DE CONTROLES		52	100	EFECTIVO

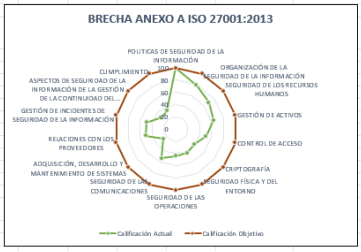

Ilustración 2 Autodiagnóstico 2025

Para el autodiagnóstico con corte a junio de 2025, se evidencia un 52% de efectividad en la evaluación de los controles. Sin embargo, llegar al 100% de la calificación objetivo aún mantiene un grado de complejidad alto, en razón a la necesidad de fortalecer el compromiso de la directicas y asignación de recursos para la implementación de controles.

De acuerdo con el reporte FURAG, las recomendaciones en lo relacionado con la seguridad y privacidad de la información para tener en cuenta en el desarrollo de este plan son las siguientes:

- Realizar pruebas de respaldo a las copias de seguridad de la información de los aplicativos misionales, estratégicos, soporte y de mejora, de manera programada para asegurar la disponibilidad de los datos en caso de Ransomware, de manera coordinada con los responsables del proceso.
- Contar con un Plan de Recuperación de Desastres -DRP-, que esté definido, documentado e implementado para todos los procesos.
- Realizar pruebas de recuperación de cada uno de los sistemas de información críticos de la entidad.
- Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) de sus infraestructuras on premise.
- Identificar y gestionar los posibles riesgos de seguridad digital (Ciberseguridad) en los servicios de Nube Pública/Privada que utiliza.
- Analizar los incidentes de seguridad digital (Ciberseguridad) que se presentaron y adoptar medidas técnicas, administrativas y de talento humano para garantizar que la seguridad digital se incorpore al plan de seguridad y privacidad de la información y así mitigar riesgos relacionados con la protección y la privacidad de la información e incidentes de seguridad digital.
- Reportar los incidentes de seguridad digital de la entidad, acorde con lo establecido en la Resolución 500 de 2022.

Como una de las actividades principales a desarrollar para la implementación de este plan, se recomienda que la Secretaría Distrital de Gobierno concientizar a la Alta Dirección del compromiso con la política de seguridad digital, y la necesidad de asignar recursos para fortalecer la implementación de controles.

2.2 Alcance

La Secretaría Distrital de Gobierno adoptará el Modelo de Seguridad y Privacidad de la Información -MSPI propuesto por MINTIC y basado en la norma ISO/IEC 27001:2022, mediante la ejecución de planes de trabajo independientes para los temas de seguridad y de privacidad de la información, por lo cual se segmentan las dependencias de la Entidad para la aplicación de los cronogramas de trabajo.

2.3 Plan de Trabajo

La Secretaría Distrital de Gobierno de Bogotá ha adoptado la Política de Seguridad de la Información, como parte del sistema integral de gestión, y para lograr su implementación y adopción ha creado un plan de seguridad de la información, con el objetivo de avanzar en la implementación orientado a dar cumplimiento a las directrices de Mintic - Ministerio de Tecnologías de Información y de las Comunicaciones, en cuanto a la adopción e implementación del Modelo de Seguridad y Privacidad de la Información.

Todas las acciones que se proponen en este plan están orientadas al fortalecimiento de la Política de Seguridad Digital como habilitador de dicha política. Así mismo, en atención tanto a lo especificado en el modelo de seguridad y privacidad, como lo estipulado en el estándar NTC ISO/IEC 27001:2022, se aborda la identificación, valoración, tratamiento y gestión de riesgos de seguridad digital, como parte fundamental del modelo y en cumplimiento en lo dispuesto en la Política de Seguridad Digital.

A continuación, se presentan las fases de implementación del Modelo de Seguridad y Privacidad de la información para la Secretaría Distrital de Gobierno de Bogotá:

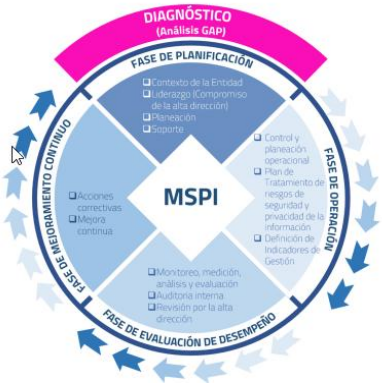

Ilustración 3 Ciclo del Modelo de Seguridad y Privacidad de la Información

Fuente: Anexo 1 Modelo de Seguridad y Privacidad de la información

2.4. Detalle de actividades del plan de trabajo según alcance y vigencia

DESCRIPCIÓN DEL PLAN						
FASE	**ACTIVIDAD**	**TAREA POR DESARROLLAR PARA EL PLAN**	**FECHA INICIO**	**FECHA FINALIZACIÓN**	**RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO**	**SEGUIMIENTO**
P	Identificación de activos	Realizar la actualización del inventario de activos de información de las localidades	Enero 2026	Julio 2026	Responsable de Seguridad de la Información	Trimestral
P	Identificación de activos	Realizar la actualización del inventario de activos de información de nivel central	Enero 2026	Julio 2026	Responsable de Seguridad de la Información	Trimestral
V	Políticas específicas de seguridad de la información	Realizar dos (2) seguimientos a los lineamientos para la implementación de la Política de Seguridad y Privacidad de la Información: uno (1) asociado a Control de acceso y otro (1) asociado a incidentes de seguridad de la información, contempladas en el Manual	Enero 2026	Diciembre 2026	Responsable de Seguridad de la Información	Semestral

Tabla con formato

DESCRIPCIÓN DEL PLAN						
FASE	**ACTIVIDAD**	**TAREA POR DESARROLLAR PARA EL PLAN**	**FECHA INICIO**	**FECHA FINALIZACIÓN**	**RESPONSABLE DEL CUMPLIMIENTO Y SEGUIMIENTO**	**SEGUIMIENTO**
		de Seguridad GDI-TIC-M004 y de acuerdo con el anexo A de la ISO 27001.				

Tabla 1~~2~~ cronograma plan de trabajo según alcance y vigencia

Tabla con formato

3. ESTRUCTURA DE MEDICION

Metas e indicadores del Plan

Para la vigencia 2026 se plantearon las siguientes metas

META	NOMBRE INDICADOR	FÓRMULA INDICADOR
Acompañar a veinte (20) alcaldías locales en la identificación, valoración y clasificación de activos, presentando el informe de avance correspondiente.	Alcaldías locales acompañadas	Número de Alcaldías locales acompañadas
Acompañar a veintitrés (23) dependencias del nivel central en la identificación, valoración y clasificación de activos, presentando el informe de avance correspondiente.	Dependencias de nivel central acompañadas	Número de dependencias de nivel central acompañadas
Realizar dos (2) seguimientos a los lineamientos para la implementación de la Política de Seguridad y Privacidad de la Información: uno (1) asociado a Control de acceso y otro (1) asociado a incidentes de seguridad de la información, contempladas en el Manual de Seguridad GDI-TIC-M004 y de acuerdo con el anexo A de la ISO 27001.	Seguimientos realizados a los lineamientos de políticas	Número de seguimientos realizados a los lineamientos de políticas

Metodología de medición

Se hará un seguimiento trimestral para determinar el nivel de cumplimiento de las metas del plan y se presentarán los avances al Comité Institucional de Gestión y Desempeño según agenda.

Periodo de implementación

El plan de seguridad y privacidad de la información se encuentra definido hasta la vigencia 2026, el cual contempla una revisión anual que puede implicar una posible reformulación de acuerdo con las nuevas directrices, normatividades distritales y nacionales y el resultado de seguimientos y auditorías internas. La ejecución del plan y el cumplimiento de las actividades se establecen para el año 2026.

4. DOCUMENTOS RELACIONADOS

Documentos internos

Código	Documento
GDI-TIC-M004	Manual de Gestión de Seguridad de la información
GDI-TIC-PL001	Plan Estratégico de las Tecnologías de la Información (PETI)
GDI-TIC-P004	Identificación y Valoración de Activos de información
GDI-DTI-P006	Procedimiento Apertura de Datos
GDI-DTI-P009	Gestión de incidentes de seguridad de la información
GDI-DTI-P010	Levantamiento del catálogo de componentes de información
GDI-TIC-F020	Formato Acuerdo de confidencialidad
GDI-TIC-F032	Formato Identificación, valoración y clasificación de activos de información
GDI-TIC-F036	Informe de incidente de seguridad de la información
GDI-TIC-F041	Acuerdo de transferencia de información

Normatividad vigente

Norma	Año	Epígrafe	Artículo(s)
Ley 1341	2009	Definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnología e Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones	Toda la norma
CONPES 3701	2011	Lineamientos de Política para Ciberseguridad y Ciberdefensa.	Toda la norma
Ley 1581	2012	Disposiciones generales para la protección de datos personales	Toda la norma
Decreto 1078	2015	Decreto único reglamentario del sector de Tecnología e Información y las comunicaciones (define el componente de seguridad y privacidad de la información)	Toda la norma
Decreto 1081	2015	"Decreto Reglamentario Único del Sector Presidencia de la República" (En especial Libro 2)	Toda la norma
Decreto 415	2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para	Toda la norma

Tabla con formato

Norma	Año	Epígrafe	Artículo(s)
		el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.	
Resolución CDS 004	2017	Fortalecimiento Institucional en Materia de TIC, para Plan Estratégico de Tecnología y Sistemas de Información (PETI) y para la Gestión de Proyectos TIC	Toda la norma
CONPES 3854	2017	Política Nacional de Seguridad Digital	Toda la norma
Decreto 1499	2017	Modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública.	Capítulo 2
CONPES 3920	2018	Política Nacional de Explotación de datos.	Toda la norma
Resolución 783	2018	Creación del Comité Institucional de Gestión y Desempeño	Toda la norma
Decreto 1008	2018	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 Tecnología e Información y las Comunicaciones.	Toda la norma
Ley 1978	2019	Moderniza el sector de las Tecnología e Información y las Comunicaciones (TIC), distribuye competencias, crea un regulador único y dicta otras disposiciones.	Articulo 22
Directiva 002	2019	Simplificación de la interacción digital entre los ciudadanos y el estado.	Toda la norma
Decreto 2106	2019	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública.	Toda la norma
Generales		Lineamientos del marco de referencia establecidos por MinTIC y que incluyen Leyes, decretos y demás desarrollos normativos que guían las acciones para implementar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI.	
Resolución 2277	2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.	Toda la norma

Documentos externos

Nombre	Año de publicación del documento y versión	Entidad que lo emite	Medio de consulta
Lineamientos PETI	2018	MINTIC	https://www.mintic.gov.co/gestionti/615/w3-article-5482.html?_noredirect=1
Ámbitos guardianes de la seguridad	2019	Alta Consejería Distrital de las TICS	http://ticbogota.gov.co/documentos/guardianes-la-informaci%C3%B3n
Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información	2025	MINTIC	https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/

Tabla con formato