2026

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARÍA DISTRITAL DE DESARROLLO ECONÓMICO

Subdirección de Informática y Sistemas

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE DESARROLLO ECONÓMICO
BOGOTÁ

TABLA DE CONTENIDO

1. INTRODUCCIÓN.

En un contexto marcado por el crecimiento exponencial de la información y la necesidad de garantizar su seguridad, el Plan de Seguridad y Privacidad de la Información 2025 de la Secretaría Distrital de Desarrollo Económico (SDDE) se plantea como una herramienta estratégica para proteger la integridad, confidencialidad y disponibilidad de los activos de información institucional.

Este plan se alinea con las disposiciones del Modelo de Seguridad y Privacidad de la Información (MSPI) y cumple con las normativas nacionales e internacionales vigentes, asegurando el cumplimiento de los estándares en materia de seguridad digital y la mitigación de riesgos asociados. Además, se integra con el Modelo Integrado de Planeación y Gestión (MIPG), fortaleciendo las capacidades institucionales para contribuir al desarrollo económico y la transformación digital del Distrito.

Es relevante destacar que el Plan Distrital de Desarrollo 2024-2027 "Bogotá Camina Segura" incluye entre sus componentes estratégicos la Seguridad Digital para el Distrito y la ciudadanía, con el objetivo de que Bogotá sea un espacio digital seguro tanto para los ciudadanos como para la administración. Este componente contempla la consolidación del equipo distrital de respuesta a incidentes cibernéticos (CSIRT), la promoción de la identificación de vulnerabilidades, la gestión de riesgos, la protección de datos personales y la prevención del cibercrimen.

Mediante una metodología estructurada, el plan define acciones concretas en diagnóstico, planificación, implementación, evaluación y mejora continua, promoviendo una cultura organizacional orientada a la protección de la información. De esta forma, se garantiza una gestión integral de riesgos que apoya la consecución de los objetivos institucionales y refuerza el compromiso de la SDDE con el desarrollo sostenible y seguro en el ámbito digital

2. DEFINICIONES Y SIGLAS

- Activos de información: es: “algo que una organización valora y, por lo tanto, debe proteger”. Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.
- Análisis de Vulnerabilidades: Identificación del nivel de exposición existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos y servidores
- CSIRT: Equipos de respuesta a incidentes de seguridad.
- Copia de seguridad: copia de datos que se realiza con el propósito de preservar la información en caso de pérdida, daño o destrucción del original
- MSPI: Modelo de Seguridad y Privacidad de la Información

3. NORMATIVIDAD

El marco normativo descrito influye en el desarrollo del plan de seguridad al proporcionar los lineamientos, estándares y directrices que las entidades deben seguir para garantizar la protección, integridad y disponibilidad de la información, así como para cumplir con la normatividad legal aplicable vigente a la SDDE.

Normatividad	Entidad	Descripción
Circular Externa No. 002 del 21 de agosto de 2024	Superintendencia de Industria y Comercio	Lineamientos sobre el tratamiento de datos personales en sistemas de inteligencia artificial
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Ley 2195 de 2022	Congreso de Colombia	Por Medio de la Cual se Adoptan Medidas en Materia de Transparencia, Prevención y Lucha Contra la corrupción Y Se Dictan Otras Disposiciones.

Normatividad	Entidad	Descripción
CONPES 4062 de 2022	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Propiedad Intelectual
Resolución 460 de 2022	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno digital, y se dictan los lineamientos generales para su implementación.
CONPES 4070 de 2021	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para la Implementación de un Modelo de Estado Abierto
Resolución 2277 de 2025	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	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.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Resolución 1519 de 2020.	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos

Normatividad	Entidad	Descripción
Resolución 2893 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se expiden los lineamientos para estandarizar ventanillas únicas, portales específicos de programas transversales, sedes electrónicas, trámites, OPA, y consultas de acceso a información pública, así como en relación con la integración al Portal Único del Estado colombiano, y se dictan otras disposiciones
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
CONPES D.C. 01 de 2019	Consejo Distrital de Política Económica y Social del Distrito Capital - CONPES D.C	Política Pública Distrital de Transparencia, Integridad y no tolerancia con la corrupción
Decreto 612 de 2018	Presidencia de la Republica	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
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano
Decreto 1078 de 2015	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones

Normatividad	Entidad	Descripción
Ley 1712 de 2014	Presidencia de la Republica	Ley de Transparencia y el Derecho a la Información Pública Nacional
Ley 1581 de 2012	Congreso de Colombia	Se dictan disposiciones generales para la protección de datos personales
CONPES 3701 de 2011.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Lineamientos de Política para Ciberseguridad y Ciberdefensa.

4. GENERALIDADES DEL PLAN O PROYECTO O PROGRAMA

4.1 Diagnóstico

Esta fase se presenta desde dos perspectivas principales: la efectividad de los controles por Dominio (ISO 27001:2022) y el avance por Componente del ciclo PHVA (Planificar, Hacer, Verificar, Actuar).
El resultado de este diagnóstico fue presentado al Comité Institucional de Gestión y Desempeño, el cual fue revisado y aprobado mediante el Acta No. 13 de 2025, sustentado en las evidencias de evaluación generadas por la herramienta de MinTIC (ver Gráfico 1: Evaluación de Efectividad de Controles – ISO 27001:2022 Anexo A).

- **Evaluación de Efectividad de Controles (ISO 27001:2022 Anexo A)**
  El promedio general se sitúa en 84.75%, indicando un buen nivel de madurez, con la necesidad de reforzar el componente tecnológico.

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES – ISO 27001:2022 ANEXO A

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	86	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	88	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	91	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	74	100	GESTIONADO
PROMEDIO EVALUACIÓN DE CONTROLES		85	100	OPTIMIZADO

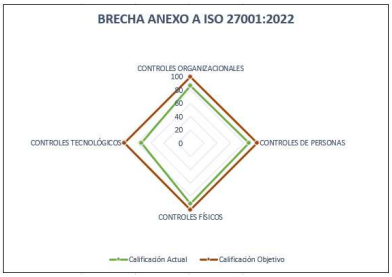

Gráfico 1: Evaluación de Efectividad de Controles (ISO 27001:2022 Anexo A)

Autodiagnostico_MSPI_SDDE_2025.xlsx – PORTADA-

- **Avance del Modelo de Operación – PHVA**
  Los componentes Planear y Hacer presentan un desempeño robusto; sin embargo, los componentes Verificar (Evaluación de desempeño) y Actuar (Mejora continua) requieren mayor estructuración.

  Esto indica que la entidad planea e implementa, pero debe fortalecer la medición, la generación de indicadores y los mecanismos formales de retroalimentación y mejora periódica.

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	**Planificación**	Contexto de la organización	14%	14%
		Liderazgo	14%	14%
		Planificación	11%	14%
		Soporte	11%	14%
	Implementación	Operación	13%	16%
	Evaluación de Desempeño	Evaluación del desempeño	11%	14%
	Mejora Continua	Mejora	11%	14%
TOTAL			**85%**	**100%**

Gráfico 2: Avance de Cláusulas del Modelo de Operación (PHVA)
Autodiagnostico_MSPI_SDDE_2025.xlsx – PORTADA-

AVANCE COMPARATIVO 2024-2025

Comparado con el diagnóstico previo consignado en el Informe Diagnóstico MSPI 2024, se evidencia un avance en la implementación del Modelo de Seguridad y Privacidad de la Información en la SDDE:

- La madurez global se incrementó de un 54% en 2024 a un 84,75% en 2025, lo que representa un aumento de 30,75 puntos porcentuales y un crecimiento relativo cercano al 57% en el nivel de cumplimiento de controles del MSPI.
- La entidad evoluciona de un nivel “Repetible” (2024) a un nivel “Gestionado/Optimizado” (2025), evidenciando que los controles ya no solo se aplican de manera parcial, sino que se encuentran más sistematizados, documentados y articulados con el modelo de operación.

- Se realizó una actualización estructural del sistema, fortaleciendo políticas, roles, matrices de control y de riesgos, así como instrumentos de evaluación y seguimiento, lo que permitió mejorar la trazabilidad y gobernanza del MSPI.
- Se incorporaron controles técnicos que no existían o no estaban formalmente gestionados en 2024, especialmente en materia de protección de la información, gestión de accesos, respaldo y manejo de incidentes, contribuyendo al aumento del nivel de cumplimiento.
- Se avanzó de manera importante en la construcción y actualización de documentos relevantes del MSPI (políticas, procedimientos, lineamientos), que hoy sirven como soporte para auditorías, comités y procesos de mejora continua.
- Pese al avance, persisten brechas en el componente tecnológico, particularmente en aspectos de desarrollo seguro, monitoreo y protección de información sensible, lo que orienta la priorización del plan de acción 2026-2027.

4.2 Objetivo(s)

Fortalecer la seguridad de la información en la Secretaría Distrital de Desarrollo Económico, asegurando la integridad, confidencialidad y disponibilidad de sus activos informativos y minimizando los riesgos asociados

4.3 Alcance

El presente Plan de Seguridad de la Información se alinea y amplía el alcance establecido en la Política de Seguridad de la Información de la Secretaría Distrital de Desarrollo Económico (SDDE). Este Plan es integral y abarca todos los procesos y procedimientos institucionales de la SDDE, enfatizando su aplicabilidad e importancia estratégica.

El alcance del Plan incluye a todos los usuarios internos y externos asociados con la SDDE. Esto comprende, pero no se limita a, servidores públicos, personal adscrito tanto a la planta permanente como provisional, contratistas, consultores, pasantes, proveedores de bienes y servicios, entidades estatales relacionadas, órganos de control y supervisión, y cualquier otro tercero que realice actividades en las instalaciones de la SDDE o en representación de esta.

Adicionalmente, el Plan se extiende a todas las formas de interacción con la información de la SDDE, incluyendo el manejo de datos en medios digitales y físicos, las comunicaciones internas y externas, y el uso de redes y sistemas informáticos. Asimismo, contempla la gestión de riesgos asociados a la seguridad de la información en todos los niveles y la promoción de una cultura organizacional que

prioriza la protección de datos y la privacidad como pilares fundamentales en todas las operaciones de la Secretaría.

4.4 Recursos

Para la ejecución del Plan de Seguridad y Privacidad de la Información 2026, la Secretaría Distrital de Desarrollo Económico dispone de los siguientes recursos, de manera general:

Recursos humanos

- Contratista de seguridad de la información.
- Profesionales de la Subdirección de Informática y Sistemas.
- Líderes de proceso y enlaces de las áreas/procesos institucionales.

Recursos tecnológicos

- Herramientas de seguridad perimetral (firewall institucional).
- Sistemas de monitoreo
- Herramientas de respaldo y restauración de la información.
- Plataformas de correo, gestor documental y servicios en Workspace

.

Recursos organizacionales

- Apoyo de la Alta Dirección.
- Comité Institucional de Gestión y Desempeño (CIGD).
- Articulación con el Modelo Integrado de Planeación y Gestión (MIPG).

5. DESCRIPCIÓN DEL PLAN, PROYECTO O PROGRAMA

En el marco de las directrices institucionales y estratégicas de la Secretaría Distrital de Desarrollo Económico, y siguiendo la metodología del Modelo de Seguridad y Privacidad de la Información (MSPI), la Subdirección de Informática y Sistemas establece un conjunto de actividades esenciales para la implementación efectiva de las estrategias de la política de seguridad y privacidad de la información. Estas actividades están alineadas con las disposiciones de la Resolución 2277 de 2025 y 500 del 2021, que define los lineamientos y estándares clave para la estrategia de seguridad digital. La adopción del MSPI no solo cumple con estos requisitos, sino que también actúa como un catalizador para habilitar y reforzar la política de Gobierno Digital de la SDDE.

Para lograr esto, se ha diseñado un plan que incluye:

5.1 Planificación

Autodiagnóstico

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Modelo de Seguridad y privacidad de la información	Actualizar el autodiagnóstico del Modelo de Seguridad y Privacidad de la Información, conforme a los lineamientos vigentes y a la Resolución 2277 de 2025.	Humano Contratista seguridad de la información
	Consolidar los resultados del autodiagnóstico y remitirlos a las instancias competentes para su revisión/aprobación	

Gestión de activos de información

Identificar los activos de información críticos de la SDDE

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Actualización activos de información 2025	Actualizar los instrumentos relacionados con la gestión de activos de información	Humano Contratista seguridad de la información
	Solicitar a los líderes de proceso la revisión y actualización de los activos de información críticos bajo su responsabilidad.	
	Validar la clasificación de la información conforme a los niveles de confidencialidad establecidos	
	Consolidar la matriz institucional de activos de información	
	Generar la versión anonimizada de la matriz de activos para su publicación, de acuerdo con la normatividad vigente	

Fuente: Elaboración propia

Gestión de riesgos de seguridad de la información

Evaluar los riesgos asociados a los activos de información críticos de la entidad, asegurando que las medidas de seguridad estén alineadas con las necesidades específicas y el entorno normativo.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Identificación, consolidación de riesgos de seguridad de la información y seguridad digital	Identificar y analizar los riesgos de seguridad de la información asociados a los activos de información críticos.	Humano Contratista seguridad de la información
	Definir controles y acciones de tratamiento acordes con la capacidad institucional.	
Seguimiento planes de tratamiento	Consolidar el plan de tratamiento de riesgos de seguridad de la información.	
	Realizar seguimiento periódico al avance de las acciones definidas.	

Fuente: Elaboración propia

Cultura organizacional y comunicación

Desarrollar programas de capacitación para concienciar a funcionarios y contratistas sobre la importancia de la seguridad y privacidad de la información, fortaleciendo la cultura de seguridad al interior de la entidad.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Cultura y apropiación	Definir una estrategia anual de sensibilización en seguridad y privacidad de la información, focalizada en los riesgos más relevantes para la entidad.	Humano Contratista seguridad de la información
Ejecución de estrategia	Divulgar lineamientos básicos sobre el manejo seguro de la información y la prevención de incidentes.	
Medición de apropiación en seguridad de la información	Ejecutar al menos una acción institucional de sensibilización dirigida a funcionarios y contratistas.	
	Documentar la ejecución y los resultados de la acción implementada.	

Fuente: Elaboración propia

Implementación

Adaptar y aplicar las políticas, procedimientos y controles establecidos en el MSPI, garantizando que estén personalizados para abordar los desafíos y objetivos de la Secretaría.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Ciberdefensa	Acompañar técnicamente el proceso de evaluación y eventual actualización de la solución de firewall institucional, sujeto a la asignación presupuestal aprobada	Humano Contratista seguridad de la información Profesional en Infraestructura
Arquitectura del sistema seguro y principios de ingeniería	Evaluar y documentar la viabilidad técnica de implementar herramientas de apoyo al análisis de código fuente, como SonarQube, para fortalecer el desarrollo seguro, sujeto a capacidades técnicas y presupuestales.	
Política de seguridad de la información	Revisar los documentos del Modelo de Seguridad y Privacidad de la Información a nivel institucional, identificando necesidades de actualización o ajuste conforme a la normatividad vigente.	
	Gestionar la validación y aprobación de los documentos actualizados por las instancias correspondientes.	
Gestión de vulnerabilidades	Estructurar y ejecutar un ciclo anual de análisis de vulnerabilidades sobre los activos tecnológicos priorizados.	
	Definir y documentar el plan de remediación correspondiente, en articulación con las áreas técnicas responsables.	

Fuente: Elaboración propia

Gestión de incidentes de seguridad de la información

Preparar y mantener procedimientos de respuesta ante incidentes de seguridad, asegurando una reacción rápida y efectiva en caso de cualquier brecha o amenaza a la seguridad de la información

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Contacto autoridades externas	Socializar con el equipo de la Subdirección de Informática y Sistemas los boletines informativos, alertas y lineamientos emitidos por dichas entidades para la prevención y gestión de incidentes de seguridad digital	Humano Contratista seguridad de la información
Documentación	Revisar y actualizar el procedimiento institucional para la gestión de incidentes de seguridad de la información, conforme a los lineamientos del MSPI y la normatividad vigente.	

Fuente: Elaboración propia

Continuidad de seguridad de la información

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Copia de seguridad de la información	Ejecutar y documentar al menos una prueba de restauración de información durante la vigencia, con el fin de validar la integridad y disponibilidad de la información respaldada.	Humano Contratista seguridad de la información
Mantenimiento y revisión	Realizar revisiones periódicas sobre los eventos y alertas generadas por las herramientas de seguridad perimetral, identificando posibles afectaciones a la disponibilidad de la información.	

Fuente: Elaboración propia

5.2 Evaluación de Desempeño

Implementar mecanismos de reporte efectivos para mantener a la alta dirección informada sobre el estado de la seguridad de la información, facilitando la toma de decisiones basada en datos y la gestión proactiva de riesgos

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Seguimiento	Reportar el seguimiento relacionado con la implementación del MSPI	Humano Contratista seguridad de la información

Fuente: Elaboración propia

5.3 Mejora Continua

Se establecen las actividades para evaluar la efectividad de las medidas de seguridad implementadas y realizar ajustes según sea necesario, manteniendo la seguridad de la información en línea con las tendencias y desarrollos tecnológicos.

LÍNEA DE ACCIÓN	ACTIVIDADES	TIPO DE RECURSO
Mejora	Documentar las acciones establecidas en los planes de mejora derivadas de revisiones internas	Humano Contratista seguridad de la información

Fuente: Elaboración propia

6. METODOLOGÍA DE SEGUIMIENTO

El seguimiento al Plan de Seguridad y Privacidad de la Información se realizará mediante un esquema articulado entre la Subdirección de Informática y Sistemas (SIS) y la Oficina Asesora de Planeación (OAP), en el cual la SIS efectuará el control interno y técnico sobre el avance de las actividades, la revisión de evidencias y el cumplimiento de los cronogramas, mientras que la OAP consolidará y reportará los resultados en el marco del Modelo Integrado de Planeación y Gestión (MIPG), permitiendo verificar el grado de ejecución, identificar desviaciones y generar insumos para la toma de decisiones y la mejora continua del plan.

7. ANEXOS

Anexo 1 PE_P7_F2_V2_ANEXO CRONOGRAMA PLAN DE SEGURIDAD

Versión	ELABORÓ	REVISÓ	APROBÓ	FECHA
1	María Alejandra Suarez Contratista Subdirección de Informática y Sistemas	Equipo MIPG- Oficina Asesora de Planeación Lady Laiton Linares Jefe Oficina Asesora de Planeación Adriana Montoya Ríos Subdirectora de Informática y Sistemas	Comité Institucional de Gestión y Desempeño (CIGD)	29/01/2026

CONTROL DE CAMBIOS			
CAMBIOS EN EL DOCUMENTO	RESPONSABLE	FECHA	VERSIÓN
Formulación y aprobación del Documento en CIGD	Adriana Montoya Ríos Subdirectora de Informática y Sistemas	29/01/2026	1

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE DESARROLLO ECONÓMICO

BOGOTÁ