Dirección de Tecnologias y Sistemas de la Información

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

TABLA DE CONTENIDO

INTRODUCCIÓN

Este documento establece las directrices, estrategias y acciones orientadas a la implementación, fortalecimiento y mejora continua de la Seguridad y Privacidad de la Información en la Secretaría de Seguridad, Convivencia y Justicia (SDSCJ) para la vigencia 2026. Su propósito es proteger los principios de Confidencialidad, Integridad y Disponibilidad de la información, en concordancia con lo dispuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en el marco de la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI).

En este contexto, la SDSCJ adopta los lineamientos y buenas prácticas aplicables a las entidades que conforman la Administración Pública, orientando la gestión de la información y de los activos tecnológicos hacia la mitigación de riesgos, el fortalecimiento de los controles y el cumplimiento de su misión institucional, contribuyendo a la eficiencia operativa y a la generación de confianza en el uso de los servicios digitales.

En este sentido, la SDSCJ define el Plan de Seguridad y Privacidad de la Información, estableciendo lineamientos que apoyan la transformación digital institucional, orientados a fortalecer la eficiencia de los procesos y el uso adecuado de las soluciones tecnologías en el desarrollo de las actividades misionales y administrativas de la Entidad.

En cumplimiento de lo dispuesto en el Decreto 612 de 2018, la actualización del presente documento define la hoja de ruta para la gestión de la seguridad de la información en la SDSCJ, alineada con los requisitos establecidos en la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022. Así mismo, se incorporan los lineamientos aplicables en materia de ciberseguridad, con el fin de fortalecer la prevención, detección y respuesta frente a posibles ciberataques que puedan afectar las soluciones y la infraestructura tecnológica de la Entidad.

OBJETIVOS

1.1. Objetivo General

Implementar y dar seguimiento a las actividades definidas en el Plan de Seguridad y Privacidad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, bajo un enfoque de mejora continua, con el fin de fortalecer la protección de las soluciones tecnológicas y los sistemas de información, en conformidad con la normativa vigente aplicable.

1.2. Objetivos Específicos

a. Implementar las acciones definidas en el plan orientadas a la apropiación y fortalecimiento de la gestión de la seguridad de la información en la Entidad, en cumplimiento de los lineamientos y requisitos establecidos en la normatividad vigente.

b. Desarrollar y consolidar las actividades establecidas, con el propósito de fortalecer progresivamente el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en la Secretaría Distrital de Seguridad, Convivencia y Justicia.

c. Fortalecer la cultura institucional en seguridad y privacidad de la información, mediante acciones de sensibilización, lineamientos y buenas prácticas dirigidas a servidores, contratistas y terceros que interactúan con la información y los activos tecnológicos de la Entidad.

ALCANCE

El Plan de Seguridad y Privacidad de la Información contempla la adopción de los controles definidos en la Norma Técnica Colombia ISO/IEC 27001:2022, mediante los cuales se promueve la implementación de buenas prácticas para la protección de la información de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

Dichas acciones se desarrollan a través del compromiso de los funcionarios, contratistas y terceros quienes, en el marco de sus responsabilidades, participan en la adopción y apropiación de las medidas de seguridad de la información establecidas por la Entidad.

CONCEPTOS TÉCNICOS

Confidencialidad: Propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, Entidades o procesos no autorizados.

Disponibilidad: Principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, Entidades o procesos autorizados

Integridad: Principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Principios de Seguridad de la información: Confidencialidad, disponibilidad e integridad.

SDSCJ: Secretaría Distrital de Seguridad Convivencia y Justicia.

MARCO NORMATIVO

El Plan Estratégico de Seguridad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta a la “Normatividad Asociada” establecido en el MA-GT-01 “Manual de Seguridad y Privacidad de la información” aprobado para la Entidad.

JUSTIFICACIÓN

El Plan de Seguridad y Privacidad de la Información fortalece la capacidad de la Secretaría Distrital de Seguridad, Convivencia y Justicia para proteger sus activos

de información mediante la implementación y mejoras del Modelo de Seguridad y Privacidad de la Información (MSPI) y el Sistema de Gestión de Seguridad de la Información (SGSI). Este plan promueve el incremento de los niveles de confidencialidad, integridad y disponibilidad de la información, en cumplimiento de la meta sectorial de la Entidad, alineada al Plan de Desarrollo Distrital.

Además, se articula con la estrategia de Gobierno Digital y se fundamenta en los lineamientos establecidos por las políticas nacionales, tales como:

- Conpes 3701 de 2011: "Lineamientos de política para ciberseguridad y ciberdefensa".
- Conpes 3854 de 2016: "Política Nacional de Seguridad Digital".
- Conpes 3975 de 2019: "Política Nacional para la Transformación Digital e Inteligencia Artificial".
- Conpes 3995 de 2020: "Política Nacional de Confianza y Seguridad Digital".

RESULTADOS ACTUALES

El análisis realizado en el año 2025, en el marco de la Evaluación del Modelo de Seguridad y Privacidad de la Información, permitió obtener una visión integral del estado de avance institucional, abarcando aspectos clave relacionados con la seguridad y privacidad de la información. Como resultado de esta evaluación, se obtuvo una calificación promedio de 87 sobre 100, lo cual refleja el compromiso institucional y los avances alcanzados en la implementación y fortalecimiento del MSPI, evidenciando un nivel de madurez sólido en la mayoría de los criterios evaluados.

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**Nivel de Madurez**
A.5	CONTROLES ORGANIZACIONALES	85	100	**OPTIMIZADO**

A.6	CONTROLES DE PERSONAS	95	100	**OPTIMIZADO**
A.7	CONTROLES FÍSICOS	86	100	**OPTIMIZADO**
A.8	CONTROLES TECNOLÓGICOS	82	100	**OPTIMIZADO**
PROMEDIO EVALUACIÓN DE CONTROLES		87	100	**OPTIMIZADO**

Tabla No. 1: Evaluación Efectividad de Controles

La identificación detallada de los ítems evaluados y de sus calificaciones actuales constituye un insumo clave para el fortalecimiento de la seguridad de la información de la Entidad. Cada uno de los ítems correspondientes a los dominios de control del instrumento de identificación de la línea base de seguridad ha sido analizado, reconociendo sus resultados como referentes para orientar acciones de mejora progresiva.

Este análisis permite establecer una línea base objetiva y priorizar iniciativas específicas, orientadas a consolidar los controles existentes, cerrar brechas identificadas y avanzar de manera estructurada en el fortalecimiento de la estrategia institucional de seguridad y privacidad de la información.

En la siguiente imagen, se complementa la información de la evaluación de efectividad de controles - ISO 27001:2022 anexo A de la norma Técnica Colombiana NTC/ISO-27001 sobre la evaluación del Modelo de Seguridad y Privacidad conforme al cierre de la vigencia 2025.

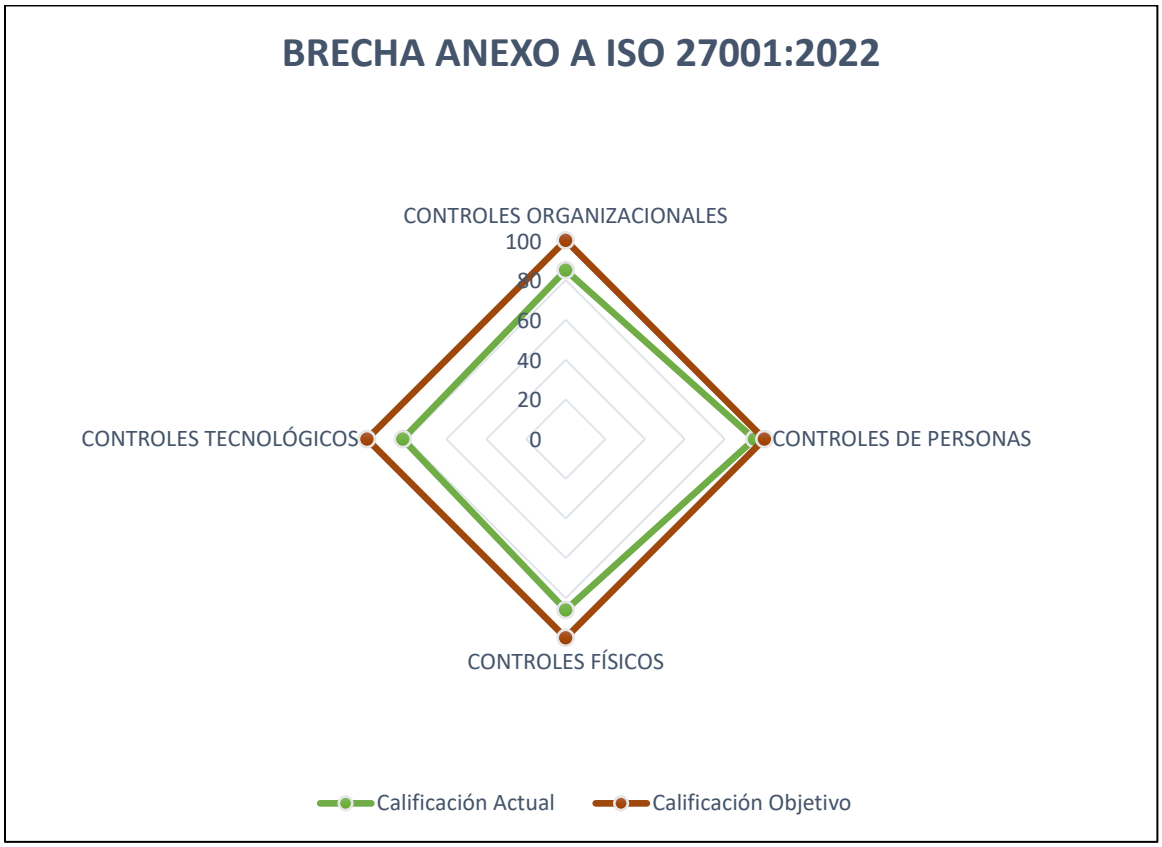

Imagen 1: Brecha Anexo A – ISO 27001

ACTIVIDADES A DESARROLLAR

A continuación, se presenta la estructura detallada que incluye las actividades, el cronograma de ejecución, los responsables asignados y los participantes involucrados, con el objetivo de facilitar y garantizar la transparencia en la implementación del Plan de Seguridad y Privacidad de la Información:

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN	META	INDICADOR	TIPO INDICADOR
1	Actualizar la documentación asociada a la seguridad y privacidad de la información.	Actualización y publicación de los documentos relativos a la seguridad de la información.	Dirección de Tecnologías y Sistemas de la Información	01/01/2026	31/12/2026	Documentos actualizados y aprobados de seguridad de la información.	(Número de documentos aprobados y actualizados / Numero de documentos planeados) *100	Eficacia
2	Actualización de la política de seguridad	Actualizar y Socializar la política de seguridad y privacidad de la información incorporando los lineamientos vigentes aplicables.	Dirección de Tecnologías y Sistemas de la Información	01/08/2026	31/12/2026	Política de Seguridad y Privacidad de la Información Actualizada	Política de Seguridad y Privacidad de la Información Actualizada	Eficacia
3	Realizar la gestión de cambios sobre las soluciones y la Infraestructura Tecnológica de la Entidad.	Gestionar los cambios asociados a las soluciones y a la infraestructura tecnológica de la Entidad, conforme a lo establecido en el procedimiento de gestión de cambios, mediante la	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Numero de Cambios presentados y gestionados.	(Número de cambios ejecutados. / Número de solicitudes de cambio presentadas) * 100.	Eficacia

		adecuada evaluación, autorización, implementación y registro de los mismos.						
4	Actualizar y publicar el Manual de Seguridad y Privacidad de la Información	Realizar la actualización y seguimiento periódico del Manual de Seguridad y Privacidad de la Información de la SDSCJ.	Dirección de Tecnologías y Sistemas de la Información	01/08/2026	31/12/2026	(1) Manual de Seguridad y Privacidad de la Información actualizado	Manual de Seguridad y Privacidad de la Información actualizado	Eficacia
5	Realizar el seguimiento a la implementación de los controles de seguridad de la información.	Validar, ajustar y fortalecer la aplicación de los controles del Anexo A de la Norma ISO/IEC 27001:2022, en concordancia con los requisitos vigentes de la Entidad.	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Número de controles implementados y verificados	(Número de Controles Implementados / Número de Controles que se planearon implementar) * 100	Eficacia
6	Apoyar en los reportes y/o requerimientos de información en cumplimiento de la Política de Gobierno Digital.	Participar en las mesas de trabajo y elaboración de reportes de información de conformidad a lo requerido en la Política de Gobierno Digital.	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Reportes de información realizados	(Número de reportes de información realizados / Número de reportes de información requeridos) * 100	Eficacia
7	Sensibilización, socialización y divulgación.	Apoyar en la ejecución de las actividades definidas en el	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Actividades de divulgación y socialización realizadas de acuerdo con lo	(Número de actividades divulgación y socialización realizadas / número de actividades divulgación y	Eficacia

		plan de uso y apropiación en lo referente a seguridad de la información.				definido en el plan de uso y apropiación.	socialización planeadas) *100	
8	Apoyar la gestión de incidentes de seguridad de la información	Gestionar los incidentes de seguridad de la información mediante la aplicación de los procedimientos establecidos y el registro de eventos en la plataforma Services Manager.	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Gestión de Incidentes de Seguridad de la Información.	(Número de incidentes atendidos / número de incidentes registrados en Services Manager *100	Eficacia
09	Reportar Trimestralmente Avances del Plan de Seguridad y Privacidad de la Información	Generar y consolidar evidencias del cumplimiento del Plan de Seguridad y Privacidad de la Información	Dirección de Tecnologías y Sistemas de la Información	01/02/2026	31/12/2026	Reporte Trimestral de actividades del Plan de Seguridad y Privacidad de la Información.	Reporte Trimestrales de actividades actualizado	Eficacia
10	Actualizar el Plan de Seguridad y Privacidad de la Información vigencia 2027.	Actualizar el Plan de Seguridad y Privacidad de la Información.	Dirección de Tecnologías y Sistemas de la Información	01/09/2026	31/12/2026	Plan de Seguridad y Privacidad de la Información actualizado	Plan de Seguridad y Privacidad de la Información actualizado.	Eficacia

Elaboró: Diego Mauricio Usme González – Contratista SDSCJ.

Revisó: Jairo Alonso Bohórquez Blanco – Profesional Especializado 222-27.
Francisco Javier Vargas Moncada - Profesional Universitario 219-18.
Diana Camila Méndez Restrepo – Contratista SDSCJ
Diana Carolina Hernandez – Contratista SDSCJ
Edwin Castillo – Contratista SDSCJ.
Jorge Eliecer Velásquez Perilla – Contratista SDSCJ.
Rafael Humberto López Saavedra – Contratista SDSCJ.
Zuleima Astrith Mancera Silva – Contratista SDSCJ.

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co