# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

## 2025

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

## TABLA DE CONTENIDO

## INTRODUCCIÓN

El presente documento establece los lineamientos, estrategias y actividades para garantizar la seguridad y privacidad de la información en la SDSCJ durante el año 2025, con el objetivo de asegurar la Confidencialidad, Integridad y Disponibilidad de la información, conforme a lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en el marco de la Política de Gobierno Digital, se implementan los lineamientos aplicables a las entidades de la Administración Pública.

En cumplimiento de esta política, las entidades estatales implementan estrategias de gestión que promueven su eficiencia operativa y el logro de su misión institucional.

En este contexto, la Secretaría de Seguridad Convivencia y Justicia implementó la Política de Seguridad y Privacidad de la Información conforme a la normativa actual, definiendo lineamientos en el marco de la transformación digital para optimizar la eficiencia de los procesos y reducir los riesgos asociados al uso de tecnologías de la información y las comunicaciones en las actividades diarias de la Entidad.

En cumplimiento a lo establecido en el Decreto 612 de 2018, en la actualización del presente documento se define la hoja de ruta a seguir en la SDSCJ en lo referente a seguridad de la información de conformidad a lo establecido en la Norma Técnica Colombiana – NTC-ISO/IEC: 27001:2022. Así mismo, se incorpora lo aplicable en materia de ciberseguridad para proteger anticipadamente o defenderse de ciberataques a las soluciones e infraestructura tecnológica de la Entidad.

## OBJETIVOS

### 1.1. Objetivo General

Ejecutar las actividades descritas en el Plan de Seguridad y Privacidad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia con un enfoque de mejora continua, que permita proteger y salvaguardar las soluciones tecnologías y sistemas de información en conformidad con la normativa aplicable.

### 1.2. Objetivos Específicos

a. Ejecutar las acciones definidas en el plan para la implementación y apropiación de la gestión de la seguridad de la información en la Entidad, cumpliendo con lo requerido en la normatividad vigente.

b. Ejecutar las actividades requeridas, con el fin de incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información en la Secretaría Distrital de Seguridad, Convivencia y Justicia.

c. Sensibilizar y/o capacitar a los funcionarios y contratistas de la Entidad en lo relacionado a seguridad de la Información, fomentando una cultura institucional, en cuanto a la necesidad de preservar los activos de información de la Entidad.

## ALCANCE

El Plan de Seguridad y Privacidad de la Información contempla los controles definidos en la Norma Técnica Colombia ISO/IEC 27001:2022, mediante el cual se implementan buenas prácticas para salvaguardar toda la información de la Secretaría Distrital de Seguridad, Convivencia y Justicia a través del compromiso de los funcionarios y contratistas mediante la adopción y apropiación de medidas de seguridad de la información.

## CONCEPTOS TÉCNICOS

**Activo de información:** Se refiere a cualquier información o elemento que tiene valor estratégico para los procesos de negocio de la Entidad. (Sistemas, soportes, edificios, hardware, recurso humano).

**Amenaza:** Según [MinTIC [1]]: causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

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

**Control:** Toda actividad o proceso encaminado a mitigar o evitar un riesgo.

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

**Impacto:** Resultado de un incidente de seguridad de la información.

**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.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**SDSCJ**: Secretaría Distrital de Seguridad Convivencia y Justicia.

[1] (S/f). Gov.co. Recuperado el 28 de diciembre de 2024, de https://gobiernodigital.mintic.gov.co/692/articles-150516_G7_Gestion_Riesgos.pdf

## MARCO NORMATIVO

El plan de seguridad y Privacidad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta al Ítem 4 “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 2024 sobre la Evaluación del Modelo de Seguridad y Privacidad ofrece una perspectiva integral del estado actual, que abarcan áreas clave para la protección de la seguridad y la privacidad en distintos contextos. Como resultado de esta revisión, se obtuvo una calificación promedio de 89 sobre 100, destacando el compromiso y los significativos avances en la gestión y fortalecimiento de estos ámbitos, lo que evidencia un desempeño sólido en la mayoría de los aspectos evaluados.

| 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** | **GESTIONADO** |

Tabla No. 1: Evaluación de 14 Dominios de Control

La identificación detallada de los ítems evaluados y sus calificaciones actuales constituye un elemento fundamental en la estrategia para reforzar la seguridad digital de la Entidad. Cada uno de los ítems dentro de los 14 dominios de control ha sido examinado, y sus puntuaciones se han reconocido como aspectos clave para impulsar la mejora continua. Este análisis minucioso establece los cimientos para implementar acciones específicas y orientadas a fortalecer la estrategia de seguridad digital.

En la siguiente imagen, se complementa la información de la brecha del anexo A de la norma Técnica Colombiana ISO-27001 sobre la evaluación del Modelo de Seguridad y Privacidad conforme al cierre de la vigencia 2024.


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 | Documentar y aprobar los procedimientos y/o documentos relacionados con seguridad de la Información | Realizar publicación de los procedimientos y/o documentos de seguridad de la información. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2025 | 31/12/2025 | 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 Modificar la política de seguridad y privacidad de la información para incluir las nuevas directrices de la Norma ISO/IEC 27001:2022. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2025 | 31/12/2025 | Política de Seguridad y Privacidad de la Información Actualizada | Política de Seguridad y Privacidad de la Información Actualizada | Eficacia |
| 3 | Ejecutar gestión de cambios a las soluciones e Infraestructura Tecnológica. | Gestión los cambios a las soluciones e infraestructura tecnológica de la Entidad de acuerdo con lo establecido en el procedimiento de | Dirección de Tecnologías y Sistemas de la Información | 01/02/2025 | 31/12/2025 | Numero de Cambios presentados y gestionados. | (Número de cambios ejecutados. / Número de solicitudes de cambio presentadas) * 100. | Eficacia |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | gestión de cambios. | | | | | | |
| 4 | Actualizar, publicar el Manual de Seguridad y Privacidad de la Información según los nuevos requisitos de la Norma ISO/IEC 27001:2022. | 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 | 01/02/2025 | 31/12/2025 | (1) Manual de Seguridad y Privacidad de la Información actualizado | Manual de Seguridad y Privacidad de la Información actualizado | Eficacia |
| 5 | Realizar validación y ajustes a la implementación de los controles según los nuevos requisitos de la Norma ISO/IEC 27001:2022. | Validar y ajustar la aplicación de los controles del anexo A de la norma ISO 27001:2022.<br>Continuar con la implementación de los controles según los nuevos requisitos de la Norma ISO/IEC 27001:2022. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2025 | 31/12/2025 | 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 | 01/02/2025 | 31/12/2025 | 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 | 01/02/2025 | 31/12/2025 | 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 | Aprobar e implementar lo definido en ciberseguridad 2024 en la Entidad de acuerdo con la aprobación de recursos. | Aprobación e implementación de las acciones a seguir de acuerdo con lo establecido en materia de ciberseguridad. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2025 | 31/12/2025 | Actividades de implementación realizadas de ciberseguridad. | (Número de actividades ejecutadas relacionadas con Ciberseguridad / número de actividades planeadas relacionadas con Ciberseguridad) *100 | Eficacia |
| 9 | Actualizar el Plan de Seguridad y Privacidad de la Información vigencia 2026. | Actualizar el Plan de Seguridad y Privacidad de la Información. | Dirección de Tecnologías y Sistemas de la Información | 01/09/2025 | 31/12/2025 | 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: Diana Camila Méndez Restrepo – Contratista SDSCJ.
Armando Alfonso Leyton Gonzalez – 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