# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

# 2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

## TABLA DE CONTENIDO

## INTRODUCCIÓN

En aras de garantizar los principios de Confidencialidad, Integridad, y Disponibilidad de la información, de conformidad a lo definido por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en el marco de la Política de Gobierno Digital, se adoptan los lineamientos a ejecutar y/o aplicar por las entidades de la Administración Pública.

En observancia de dicha política, las entidades estatales desarrollan estrategias de gestión que facilitan su óptimo funcionamiento y el cumplimiento de la misión institucional.

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, estableciendo directrices 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.

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: 27001:2013. 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.

# 1. OBJETIVOS

## 1.1. Objetivo General

Ejecutar el Plan de Seguridad y Privacidad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, bajo un enfoque de mejora continua que permita salvaguardar la tecnologías y sistemas de información en cumplimiento a la normatividad vigente.

## 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.

## 2. ALCANCE

El Plan de Seguridad y Privacidad de la Información contempla los controles definidos en la Norma Técnica Colombia ISO IEC 27001:2013, 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.

## 3. 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 [ISO/IEC 13335-1:2004[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. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

**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.

[1] Information technology — Security techniques — Management of information and communications technology security

**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.

## 4. 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” versión 4 aprobado para la Entidad.

## 5. JUSTIFICACIÓN

El Plan de seguridad y privacidad de la Información contribuye a que la Secretaría Distrital de Seguridad, Convivencia y Justicia, por medio de la implementación del Modelo de Seguridad y Privacidad de Ia Información - MSPI y la Gestión de Seguridad y Privacidad de la Información – SGSI, incremente los niveles de confidencialidad, integridad y disponibilidad de la información en cuanto a la necesidad de preservar los activos de información de la Entidad, en cumplimiento a lo definido en la Meta sectorial de la Entidad "Implementar el 50% de la Política de Seguridad Digital acorde a la normativa Distrital y Nacional en la Secretaría de Seguridad, Convivencia y Justicia", la cual está alineada al Plan de Desarrollo Distrital, así como lo definido en la estrategia de Gobierno Digital, lo propuesto desde los Conpes 3701 del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”, 3854 del 2016 Política Nacional de Seguridad Digital, 3975 del 2019 “Política Nacional para la Transformación Digital e Inteligencia Artificial” y 3995 del 2020 “Política Nacional de Confianza y Seguridad Digital”.

## 6. RESULTADOS ACTUALES

Dentro del análisis del año 2023 sobre la Evaluación del Modelo de Seguridad y Privacidad, se presenta el estado actual que proporciona una visión integral de los 14 dominios de control. Estos dominios abarcan un espectro amplio de aspectos vitales para la seguridad y la protección de la privacidad en diversos entornos. Tras una revisión y evaluación, se ha logrado obtener una calificación promedio sumamente positiva de 87 puntos sobre un total de 100. Esta puntuación refleja el compromiso y los esfuerzos destacados realizados en el fortalecimiento y la gestión efectiva de los diferentes ámbitos de seguridad y privacidad, evidenciando así un sólido desempeño 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 | 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 | **EFECTIVO** |
| ***PROMEDIO EVALUACIÓN DE CONTROLES*** | | **87** | **100** | **GESTIONADO** |

Tabla No. 1: Evaluación de 14 Dominios de Control

La descripción detallada de los ítems y sus respectivas calificaciones actuales representa un paso crucial en el proceso estratégico hacia el fortalecimiento de la seguridad digital de la Entidad. Cada ítem evaluado dentro de los 14 dominios de control ha sido analizado, y sus puntuaciones actuales se han identificado como puntos clave para la mejora continua. Esta evaluación detallada sienta las bases para acciones específicas y focalizadas destinadas a potenciar 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-27001:2013 sobre la evaluación del Modelo de Seguridad y Privacidad conforme al cierre de la vigencia 2023.


Imagen 1: Brecha Anexo A – ISO 27001:2013

## 7. ACTIVIDADES A DESARROLLAR

La estructura detallada que abarca las actividades, su cronograma de ejecución, los responsables asignados y los participantes involucrados se presenta a continuación para facilitar y dar transparencia al proceso de 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 | 01/02/2024 | 30/12/2024 | 100% | (Número de documentos aprobados y actualizados / Numero de documentos planeados) *100 | Eficacia |
| 2 | Definir e implementar indicadores de Gestión de Seguridad y privacidad de la Información. | Formular, formalizar, implementar y medir la eficiencia y eficacia de los indicadores de Gestión de Seguridad y privacidad de la Información. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2024 | 30/06/2024 | 100% | (Número de indicadores definidos e implementados / Numero de indicadores planeados) *100 | 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 | 01/02/2024 | 31/12/2024 | 100% | (Número de cambios ejecutados. / Número de solicitudes de cambio presentadas) * 100. | Eficacia |

| N° | ACTIVIDAD | TAREA | RESPONSABLE | INICIO | FIN | META | INDICADOR | TIPO INDICADOR |
|---|---|---|---|---|---|---|---|---|
| | | gestión de cambios. | | | | | | |
| 4 | Actualizar, publicar y realizar seguimiento al 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 | 01/02/2024 | 30/06/2024 | Un Manual de Seguridad y Privacidad de la Información actualizado | Manual de Seguridad y Privacidad de la Información actualizado | Eficacia |
| 5 | Realizar seguimiento a la implementación de los controles del anexo A de la norma ISO 27001:2013 | Verificar la aplicación de los controles en la SDSCJ del anexo A de la norma ISO 27001:2013.<br>Continuar con la implementación de los controles en la SDSCJ del anexo A de la norma ISO 27001:2013. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2024 | 31/12/2024 | 100% | (Número de Controles Implementados / Número de Controles que se planeados) * 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 | 01/02/2024 | 31/12/2024 | 3 | (Número de reportes de información realizados / Número de reportes de información planificados) * 100 | Eficacia |
| 7 | Apoyar en las actividades requeridas para la socialización | Apoyar en la ejecución de las actividades definidas en el | Dirección de Tecnologías y Sistemas de la Información | 01/02/2024 | 31/12/2024 | 3 | (Número de actividades divulgación y socialización realizadas / número de actividades divulgación y | Eficacia |

| N° | ACTIVIDAD | TAREA | RESPONSABLE | INICIO | FIN | META | INDICADOR | TIPO INDICADOR |
|---|---|---|---|---|---|---|---|---|
| | y divulgación de temas de seguridad de la información. | plan de uso y apropiación en lo referente a seguridad de la información . | | | | | socialización planeadas) *100 | |
| 8 | Analizar, identificar e implementar lo aplicable en ciberseguridad en la Entidad. | Efectuar el Análisis del estado actual y definir las acciones a seguir de acuerdo a lo establecido en materia de ciberseguridad. | Dirección de Tecnologías y Sistemas de la Información | 01/02/2024 | 31/12/2024 | 100% | (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 2025. | Actualizar el Plan de Seguridad y Privacidad de la Información. | Dirección de Tecnologías y Sistemas de la Información | 01/09/2024 | 31/12/2024 | Un 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.
Adriana del pilar Monroy Cubillos – Contratista SDSCJ.
Edwin Castillo Ortiz – Contratista SDSCJ.
Francisco Javier Vargas Moncada - Profesional Universitario 219-18.
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