PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

TABLA DE CONTENIDO

1.INTRODUCCIÓN

Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en aras de garantizar los principios de Integridad, confidencialidad y disponibilidad de la información, establece la Política de Gobierno Digital, a través de la cual genera 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 y la continuidad del negocio.

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 a 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.

Para lo cual, por medio del presente documento se define la hoja de ruta a seguir en el SDSCJ acorde a lo establecido en la Norma Técnica Colombiana - NTC – ISO – IEC: 27001:2013 aplicando el ciclo de mejora continua y lo establecido para la gestión de seguridad y privacidad de la Información en la vigencia 2023, en cumplimiento a lo establecido en el Decreto 612 de 2018.

2.OBJETIVOS

2.1. Objetivo General

Desarrollar e implementar 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 confidencialidad, integridad y disponibilidad de la información en cumplimiento a la normatividad vigente y el aseguramiento de la información como el activo más significativo de la Entidad.

2.2. Objetivos Específicos

a. Ejecutar las acciones para implementación y apropiación del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, con el objetivo de salvaguardar la información

b. 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 a los funcionarios y contratistas de la Entidad acerca del Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, fomentando una cultura institucional, en cuanto a la necesidad de preservar los activos de información de la Entidad.

d. Hacer uso eficiente y seguro de los recursos de TI en la Secretaría Distrital de Seguridad, Convivencia y Justicia (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.

3.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.

4. 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.

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

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

SDSCJ: Secretaría Distrital de Seguridad Convivencia y Justicia.

SGSI: Sistema de Gestión de Seguridad de la Información.

5.MARCO NORMATIVO

El plan de seguridad y Privacidad de la Información de la Secretaría Distrital Seguridad, Convivencia y Justicia se ajusta al Ítem 4 “Marco Legal” establecido en el MA-GT-01 “Manual de Seguridad y Privacidad de la información” versión 3 aprobado para la Entidad.

6.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 Sistema de 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”.

7.RESULTADOS ACTUALES

En la siguiente tabla, se presenta el estado actual de la evaluación de los 14 dominios de control de la Evaluación del Modelo de Seguridad y Privacidad para el año 2022, con una calificación promedio de 85/100.

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	93	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	84	100	**OPTIMIZADO**
A.12	SEGURIDAD DE LAS OPERACIONES	88	100	**OPTIMIZADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	80	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	77	100	**GESTIONADO**
A.18	CUMPLIMIENTO	76,5	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**85**	**100**	**GESTIONADO**

Tabla No. 1: Evaluación de 14 Dominios de Control

Se describen los ítems con la calificación actual, con el fin de adelantar las acciones para el fortalecimiento de la estrategia de seguridad digital de la Entidad.

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 2022.

Imagen 1: Brecha Anexo A – ISO 27001:2013

8.ACTIVIDADES A DESARROLLAR

El detalle de las actividades a realizar, tiempo de ejecución de las mismas, responsable y participantes, para adelantar la implementación de este plan se puede referenciar a continuación:

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN
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	01/02/2023	30/11/2023
2	Definir e implementar indicadores del sistema de Gestión de Seguridad y privacidad de la Información.	Formular, formalizar, implementar y medir la eficiencia y eficacia de los indicadores del sistema de Gestión de Seguridad y	Dirección de Tecnologías y Sistemas de la Información	01/02/2023	30/06/2023

N°	ACTIVIDAD	TAREA	RESPONSABLE	INICIO	FIN
		privacidad de la Información.			
3	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	01/07/2023	30/09/2023
4	Realizar seguimiento a la implementación de los controles del anexo A de la norma ISO 27001:2013	Avanzar en la implementación de los controles aplicables a la SDSCJ del anexo A de la norma ISO 27001:2013	Dirección de Tecnologías y Sistemas de la Información	01/02/2023	30/11/2023
5	Apoyar el cumplimiento de la Política de Gobierno Digital	Apropiar el Marco de Referencia de “Política de Gobierno Digital”	Dirección de Tecnologías y Sistemas de la Información	01/02/2023	30/11/2023
6	Incorporar actividades de socialización y divulgación de temas de seguridad de la información en el Plan de Uso y Apropiación de la DTSI.	Ejecutar el plan de entrenamientos en temas relacionados con temas relacionados con seguridad de la información	Dirección de Tecnologías y Sistemas de la Información	01/02/2023	30/11/2023
7	Realizar ejercicio de simulación de incidentes seguridad Digital al interior de la Entidad.	Realizar ejercicios de simulación de incidentes para desarrollar habilidades y destrezas en materia de seguridad digital al interior de la Entidad.	Dirección de Tecnologías y Sistemas de la Información	01/03/2023	30/11/2023
8	Definir, y aprobar la Política de Ciberseguridad de la Entidad	Definir formalizarla política de Ciberseguridad de la Entidad	Dirección de Tecnologías y Sistemas de la Información	01/02/2023	31/11/2023

9.CONTROL DE CAMBIOS

Fecha	Versión	Descripción
23/07/2018	1	Creación del Documento
12/08/2019	2	Actualización de contenidos en: Glosario de términos; inclusión de términos; Marco legal; inclusión de normas; cronograma de implementación de acuerdo a plan de trabajo 2019
20/01/2020	3	Actualización cronograma de implementación plan de seguridad de la información 2020.
13/03/2020	4	Se ajustan logos de Alcaldía y de la Certificación ISO 9001-2015 Calidad.
31/08/2021	5	Actualización de contenidos en: Marco legal; inclusión de normas, Cronograma de Implementación 2020, para el segundo semestre.
21/10/2021	6	Por solicitud de la Dirección de Tecnologías y Sistemas de la Información de la SDSCJ se ajusta nuevamente y se actualiza el documento.
08/07/2021	7	Elaboración del Plan de Seguridad y Privacidad de la Información 2021, aprobado en la sesión del 08 de Julio del 2021 de la Mesa Técnica de Seguridad Digital.
30/01/2022	8	Elaboración del Plan de Seguridad y Privacidad de la Información 2022.
26/01/2023	9	Elaboración del Plan de Seguridad y Privacidad de la Información 2023.

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