PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

DIRECTOR

FABIO DE JESÚS VILLA RODRÍGUEZ
Director Escuela Contra La Drogadicción

PREPARÓ

GERARDO VANEGAS JARAMILLO
Subdirector Administrativo y Financiero

VIGENCIA 2023

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 GobiernoDigital, 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 Escuela Contra La Drogadicción, 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 la Entidad.

Para lo cual, por medio del presente documento se define la hoja de ruta a seguir 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 2022, encumplimiento 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 Escuela Contra La Drogadicción - ECD, 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

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

Incrementar el nivel de madurez del Modelo de Seguridad y Privacidad de laInformación en la ECD.

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.

Hacer uso eficiente y seguro de los recursos de TI en la Escuela Contra La Drogadicción (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 Escuela Contra La Drogadicción - ECD 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).
DATOS: Corresponde a los elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la ECD.
PERSONAL: Corresponde a todo el personal de la ECD, funcionarios, contratistas, clientes, usuarios finales y en general, todos aquellos quetengan acceso de una manera u otra a los activos de información de la ECD.
SERVICIOS: Corresponde a cualquier tipo de servicios interno o externo suministrados por la Entidad a una parte interesada.
TECNOLOGÍA: Corresponde a los equipos, sistemas de información, procesos y procedimientos utilizados para gestionar la información y las comunicaciones.

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.
ANÁLISIS DE RIESGOS: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.
AUTORIZACIÓN: Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos delsistema de información o activos físicos.

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. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas y que pueden ser de carácter administrativo, técnico o legal. En la entidad se aplica por medio de la declaración de aplicabilidad.
CRITICIDAD: Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
DESASTRE: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
DESVIACIÓN (SEGURIDAD DE LA INFORMACIÓN): Malas prácticas adelantadas por las personas y que generan posibles incidentes o riesgos.
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.

INVENTARIO DE ACTIVOS: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

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 lainformación.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN: Confidencialidad, disponibilidad e integridad.

SEGURIDAD DE LA INFORMACIÓN: Consiste en resguardar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja laEntidad, mediante un conjunto de medidas preventivas y correctivas.

SERVICIO: Cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

5.MARCO NORMATIVO

El Plan de Seguridad y Privacidad de la Información, considera entre otros el siguiente marco normativo:

a. LEY 1978 de 2019: "*Por la cual se moderniza el sector de las tecnologías de la información y las comunicaciones -TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones*"

b. LEY 1955 de 2019: "*Por la cual se expide el Plan Nacional de Desarrollo, enlos artículos 147 y 148 se establece lo referente a la Transformación Digital Pública y Gobierno Digital como política de gestión y desempeñoInstitucional"*

c. LEY 1273 de 2009: "*Por la cual se modifica el Código Penal, se crea un nuevobien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."*

d. LEY 1341 de 2009. "*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de laInformación y las Comunicaciones –TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones*

e. DECRETO 806 de 2020: *Por el cual se adoptan medidas para implementar las tecnologías de la información y las comunicaciones en las actuaciones judiciales, agilizar los procesos judiciales y flexibilizar la atención a los usuarios del servicio de justicia, en el marco del Estado de Emergencia Económica, social y ecológica*.

6. JUSTIFICACIÓN

El Plan de seguridad y privacidad de la Información contribuye a que la Escuela Contra La Drogadicción, por medio de la implementación 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 fomentando una cultura institucional, 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 30% de la Política de Seguridad Digital acorde a una meta inicial,* 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.ESTADO ACTUAL

De acuerdo a los resultados promedio del 31 % de acuerdo a la Evaluación del Modelo de Seguridad y Privacidad para el año 2022, se describen los ítems con la calificación actual, con el fin de que se adelanten las acciones para el fortalecimientode la estrategia de seguridad digital de la Entidad:

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	80	100	**GESTIONADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	20	100	**NO EFECTIVO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	40	100	**NO EFECTIVO**
A.8	GESTIÓN DE ACTIVOS	17	100	**NO EFECTIVO**
A.9	CONTROL DE ACCESO	20	100	**NO GESTIONADO**
A.10	CRIPTOGRAFÍA	0	100	**NO GESTIONADO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	19	100	**NO EFECTIVO**
A.12	SEGURIDAD DE LAS OPERACIONES	22	100	**NO GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	24	100	**NO GESTIONADO**

No.	Evaluación de Efectividad de controles			
	DOMINIO	**Calificación Actual**	**Calificación Objetivo**	**EVALUACIÓN DE EFECTIVIDAD DE CONTROL**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	20	100	**NO EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	60	100	**EFECTIVO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	21	100	**NO GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54	100	**EFECTIVO**
A.18	CUMPLIMIENTO	40	100	**EFECTIVO**
PROMEDIO EVALUACIÓN DE CONTROLES		**31**	**100**	**NO GESTIONADO**

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	FECHA DE INICIO	FECHA FIN
1	Definir roles y responsabilidades de seguridad y privacidad de la información	Definir roles y responsabilidades de los funcionarios y contratistas en relación a Seguridad de la Información	Dirección de Tecnologías y Sistemas de la Información	1/02/2023	31/03/2023
2	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	1/02/2023	31/03/2023
3	Desarrollar la Matriz de Servicios Internos Tecnológicos de la Información.	Apropiación matriz de servicios internos tecnológicos de la información	Dirección de Tecnologías y Sistemas de la Información	1/03/2023	1/08/2023
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	1/02/2023	28/02/2023
5	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	1/04/2023	30/04/2023
6	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	1/04/2023	30/04/2023
7	Plan de Uso y Apropiación	Ejecutar el plan de entrenamientos en temas relacionados con temas relacionados con seguridad de la información	Dirección de Tecnologías y Sistemas de la Información	1/03/2023	31/03/2023

9. CONTROL DE CAMBIOS

Fecha	Versión	Descripción
23/11/2022	1	Creación del Documento

10. BIBLIOGRAFÍA

VERSIÓN ACTUALIZADA DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARIA DE SEGURIDAD Y JUSTICIA DE BOGOTÁ