PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2025 SED

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Vigencia 2025

Tabla de Contenido

1. JUSTIFICACIÓN 5
2. METODOLOGÍA 5
3. OBJETIVO 6
4. ALCANCE 6
5. ÁMBITO DE APLICACIÓN 7
6. PLAN DE ACCIÓN 7
   - 6.1. Fase de Planeación 7
   - 6.2. Fase de Implementación 8
   - 6.3. Fase de Verificación 8
   - 6.4. Fase Mejora Continua 9

GLOSARIO

ACTIVOS: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

ACTIVO DE INFORMACIÓN: bien de la entidad (representado en su información y datos) que tiene valor para los procesos de negocio, independientemente de su ubicación; puede ser un documento físico debidamente firmado, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información valiosa o útil.

AMENAZAS: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a 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.

AUDITORÍA: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000)

CIBERSEGURIDAD: protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa almacena y transporta mediante los servicios de información que se encuentran interconectados.

CONTINUIDAD: la continuidad es el proceso de establecer por adelantado, las capacidades necesarias para evitar o mitigar el impacto de un acontecimiento que provoca la interrupción de las operaciones en una o más procesos.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: es 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.

CONTROL DE ACCESO: una característica o técnica en un sistema de comunicaciones para permitir o negar el uso de algunos componentes o algunas de sus funciones.

DISPONIBILIDAD: la disponibilidad consiste en asegurarse que los usuarios autorizados tengan acceso a la información y a los sistemas de apoyo, cuando se requiera, se trata de la propiedad de ser accesible y utilizable, bajo solicitud por una entidad autorizada.

GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

ISO/IEC 27001:2022: norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

MEDIOS DE ALMACENAMIENTO DIGITAL: son todos aquellos dispositivos autorizados por la Secretaría de Educación del Distrito, que permiten el almacenamiento de información, los cuales pueden ingresar o salir de las instalaciones de la entidad con la respectiva autorización. Se incluyen equipos portátiles, teléfonos inteligentes, Ipods, reproductores mp3, memorias USB/SD/Mini-SD, CDs, DVDs, cintas: respaldo y similares. Asimismo, se incluyen correos electrónicos y conexiones por donde pueda ser transportada la información de la Entidad.

MEDIO REMOVIBLE: medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, diskettes, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

PLAN DE TRATAMIENTO DE RIESGOS: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000)

PROCEDIMIENTO: los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la organización, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

RIESGO: efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital. (ISO/IEC 27000).

SEGURIDAD DIGITAL: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales.

SENSIBILIDAD: nivel de impacto que una divulgación no autorizada podría generar.

SERVICIO: es 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.

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

VULNERABILIDAD: debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

1. JUSTIFICACIÓN

La Secretaría de Educación del Distrito trabaja para garantizar el derecho de los niños, niñas y jóvenes de Bogotá a una Educación de Calidad, basada en el aprendizaje integral para el buen vivir, la excelencia académica, la inclusión y la equidad. Nuestros procesos se llevan a cabo buscando la satisfacción de la comunidad educativa: estudiantes, padres de familia, docentes, orientadores y directivos docentes.

En la SED fomentamos la educación de calidad, manteniendo la confidencialidad, integridad y disponibilidad de los activos de información soportados en la innovación, la gestión de la documentación y la información, la gestión del conocimiento, la evaluación y el autocontrol.

El Modelo de Seguridad y Privacidad de la Información del Sistema deGestión de Seguridad de la Información de la SED, busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información

Este documento relaciona la información detallada para implementar y mantener la Seguridad de la Información de la SED para la vigencia 2025, relacionando las actividades, para asegurar el cumplimiento de los resultados esperados.

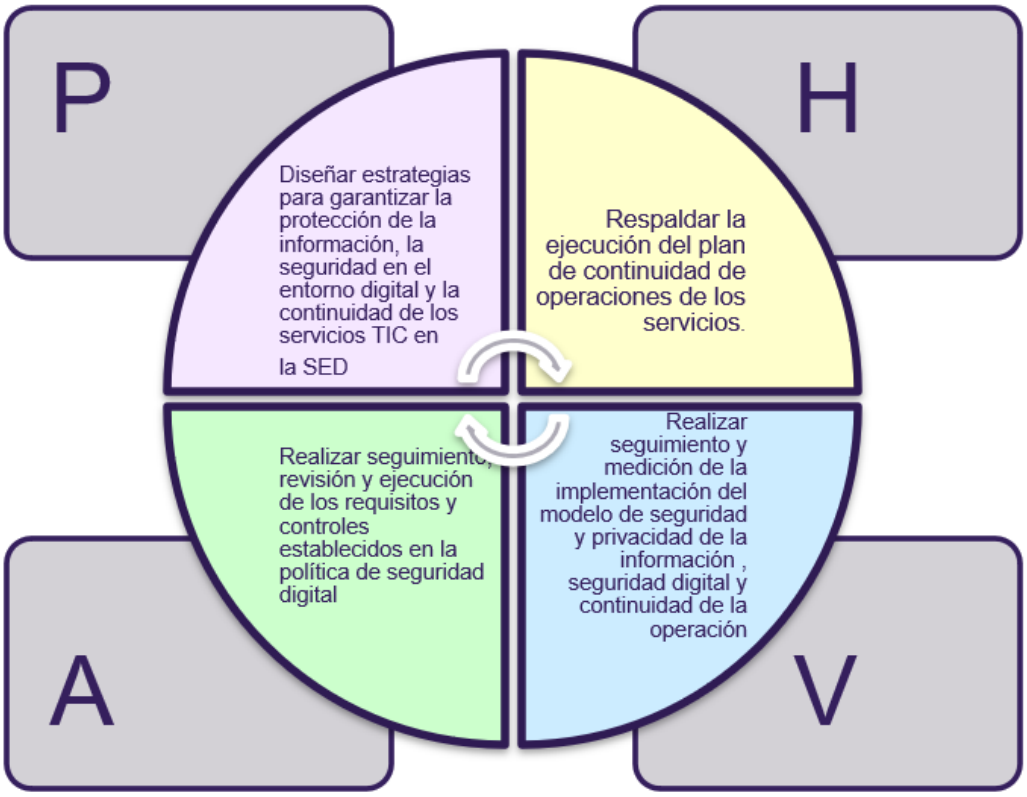
Es de resaltar que en el 2024 se logró obtener resultados importantes con la ejecución de las acciones del Plan de Seguridad y privacidad de la información 2024, entre las cuales se destacan los siguientes:

1.Actualización de la metodología para la identificación y clasificación de los activos de información, que incluyo diferentes mejoras en el instrumento, para identificar información relevante en la toma de decisiones por parte de los lideres de procesos.
2. Actualización de la metodología para el tratamiento de riesgos de Seguridad de la información
3. Articulación de las políticas de seguridad en cada uno de los dominios aplicables en la SED.
4. Fortalecimiento de la conciencia y cultura organizacional respecto a la Seguridad de la Información.
5. Fortalecimiento en la gestión y toma de conciencia de los incidentes de seguridad de la Información.

2. METODOLOGÍA

De acuerdo con el modelo indicado por el Ministerio de Tecnologías de la Información y las Comunicaciones la metodología aplicada para el plan de seguridad y privacidad de la información de la SED corresponde al ciclo PHVA (Planear, Hacer, Verificar y Actuar), tal como se visualiza en la figura 1

FIGURA 1. **CICLO PHVA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN SED.**



Fuente: Elaboración Propia

3. OBJETIVO

El Plan de Seguridad y Privacidad de la Información de la SED, busca prevenir los efectos no deseados que se puedan presentar en cuanto a seguridad de la información, con el fin de lograr niveles adecuados de integridad, confidencialidad y disponibilidad para toda la información relevante para asegurar la continuidad operacional de los procesos y servicios que presta la SED. con base en los lineamientos del Modelo de Seguridad y Privacidad de la Información los cuales están alineados con la NTC/IEC ISO 27001, las recomendaciones del FURAG frente a la implementación de la Política de Seguridad Digital y los lineamientos del Modelo Integrado de Planeación y Gestión – MIPG.

4. ALCANCE

El plan de seguridad y privacidad de la información tiene como fin mejorar la seguridad digital de todos los procesos, procedimientos y políticas de la SED en todos sus niveles (Central, local e institucional) aplicado a todos los funcionarios, contratistas, terceros y comunidad educativa que mediante sus funciones utilicen, recolecten, compartan intercambien consulten y/o procesen información a través de

cualquier medio, formato y ubicación.

5. ÁMBITO DE APLICACIÓN

El Plan de Seguridad y Privacidad de la Información, así como la Política de Seguridad Digital, aplica a todos los niveles funcionales y organizacionales de la Secretaria de Educación del Distrito, a todos sus funcionarios, contratistas, proveedores, operadores, entidades adscritas, así como aquellas personas o terceros que en razón del cumplimiento de sus funciones y las de la SED compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control, demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.
De igual manera, este plan aplica a toda la información creada, procesada o utilizada por SED, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

6. PLAN DE ACCIÓN

La Secretaría de Educación del Distrito establece el Plan de Seguridad y Privacidad de la Información mediante el cual se implementará el análisis, la ejecución y el cumplimiento de los objetivos y actividades, teniendo en cuenta los roles, responsabilidades y tiempos planteados en cada una de las siguientes fases:

6.1. Fase de Planificación

ACCION / ESTRATEGIA	PRODUCTO	2026											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
FASE PLANIFICACIÓN													
Alinear los objetivos de la seguridad de la información con los objetivos del PESI.	Plan Estratégico De Seguridad De La Información - PESI												
Elaborar matriz PESI (estimación recursos, tiempos, justificación y priorización	Matriz PESI												
Revisar y actualizar los documentos correspondientes a: - Plan de Seguridad y Privacidad de la Información - Plan de Tratamiento de Riesgos	Plan de Seguridad y Privacidad de la Información 2025 Plan de Tratamiento de Riesgos 2025												

ACCION / ESTRATEGIA	PRODUCTO	2026											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Publicación de los Planes de seguridad y privacidad de la Información, Plan de tratamiento de riesgos y el PESI	Planes publicados link de transparencia												
Revisar, actualizar y socializar en caso de ser requerido, la metodología de gestión de activos de información y el instrumento.	Metodología de activos/Instrumento actualizado												

6.2. Fase de Implementación

ACCION / ESTRATEGIA	PRODUCTO	2026											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
FASE IMPLEMENTACION													
Actualización y aprobación de activos de información.	Activos de información actualizados												
Publicación de activos de información	Activos de información publicados												
Socializaciones de la Política de Seguridad de la Información	Política de Seguridad Socializada												

6.3. Fase de Verificación

ACCION / ESTRATEGIA	PRODUCTO	2026											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
FASE: VERIFICACION													
Actualización y seguimiento de riesgos de seguridad de la Información	Mapa de riesgos de SI actualizado												
Registrar las bases de datos teniendo en cuenta la información suministrada por las áreas de los activos de información	Certificado del registro de BD que expide la SIC												

ACCION / ESTRATEGIA	PRODUCTO	2026											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
Gestionar los incidentes de seguridad de la información reportados a la mesa de ayuda	Casos de soporte gestionados de los incidentes de SI												

6.4. Fase Mejora Continua

ACCION / ESTRATEGIA	PRODUCTO	2025											
		ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
FASE MEJORA CONTINUA													
Aplicar Autodiagnóstico de la Política de Gobierno Digital	Autodiagnóstico de la Política de Gobierno Digital, según el FURAG												
Efectuar registro y seguimiento de reportes incidentes de seguridad internos de la entidad	Informes de incidentes de seguridad digital vigencia 2025												

DOCUMENTO APROBADO POR EL COMITÉ INSITUCIONAL DE GESTIÓN Y DESEMPEÑO EL 31 DE ENERO DE 2025

Elaborado: Henry Alexander Moyán Montenegro - Profesional Contratista Oficina OTIC
Cesar Ubaldo Báez Báez - Profesional Especializado Oficina OTIC
Luz Dary Vargas Suarez - Profesional Especializado Oficina OTIC
Juan Carlos Parra Moreno - Profesional Contratista Oficina OTIC

Revisado: Milena Del Pilar Sandoval Gómez Jefe OTIC
Jairo Alberto Orduz Salamanca - Profesional Especializado Oficina OTIC