ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

SECRETARÍA DE EDUCACIÓN DEL DISTRITO

12-MN-001 Manual de la Política General de Gestión de Seguridad de la Información

Versión 2

Febrero 2022

Av. Eldorado No. 66 – 63
PBX: 324 10 00
Fax: 315 34 48
http://www.educacionbogota.edu.co
Información: Línea 195

1. INTRODUCCIÓN

La Política General de Gestión de Seguridad de la Información refleja el compromiso de la alta dirección de la SED con los principios de seguridad y privacidad de la información para que la gestión pública se realice con eficiencia, transparencia, previendo riesgos, racionalizando y ofreciendo accesibilidad a sus trámites y servicios.

2. OBJETIVO DEL PRESENTE MANUAL.

La política y los lineamientos definidos en este documento se constituyen para la Secretaría de Educación del Distrito en el marco interno regulatorio del Modelo Integrado de Planeación y Gestión MIPG y la base para la planificación e implantación de los controles, procesos y procedimientos que garanticen la disponibilidad, integridad y disponibilidad de los activos de información.

3. ALCANCE DEL PRESENTE MANUAL

A través de este manual se muestra los conceptos generales, los lineamientos, responsabilidades y acciones que se deben adelantar para dar cumplimiento a la implementación de la Política General de Gestión de Seguridad de la Información de la Secretaría de Educación del Distrito.

4. DEFINICIÓN DE LA POLITICA DE SEGURIDAD DE LA INFORMACION EN EL MARCO DEL MODELO INTEGRADO DE PLANEACION Y GESTION MIPG

El Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las entidades.

Con la política se fortalecen las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, así como en la creación e implementación de instrumentos de resiliencia, recuperación y respuesta nacional en un marco de cooperación, colaboración y asistencia.

5. OBJETIVOS ESPECIFICOS DE LA POLÍTICA GENERAL DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de esta política son**:**

- Minimizar el riesgo de incumplimiento de los objetivos misionales de la entidad y de afectación de los servicios internos y externos por incidentes, fallas o vulnerabilidades.
- Cumplir con los principios generales de seguridad de la información definidos en las normas

y reglamentación vigente.

- Cumplir con los principios de la función administrativa.
- Mantener la confianza de la ciudadanía, entes de control, entidades gubernamentales en la información y servicios ofrecidos por la SED
- Gestionar los riesgos tecnológicos de la institución, cumpliendo con las normas y recomendaciones de mejores prácticas de seguridad.
- Proteger los activos de información brindando confiablidad, integridad y disponibilidad.
- Establecer el manual de la política, procesos, procedimientos e instructivos en materia de seguridad de la información al interior de la SED.
- Fortalecer la cultura de seguridad de la información sensibilizando y capacitando a los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general todas las personas que usen la información ofrecida por la entidad.
- Definir los responsables, funciones y roles en la planificación, implementación, control, seguimiento y mejoramiento de la Política de gestión de seguridad de la información.
- Garantizar la continuidad del negocio frente a incidentes.

6. ALCANCE DE LA POLITICA GENERAL DE GESTION DE SEGURIDAD DE LA INFORMACION

La Política General de Gestión de Seguridad de la Información aplica para todos los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general a todas las personas que de manera directa o indirecta hagan uso de la información ofrecida por la entidad en el nivel central, local e institucional.

7. MARCO LEGAL

El Artículo 5º del Acuerdo Distrital 257 de 2006, establece que las actuaciones administrativas serán públicas y estarán soportadas en tecnologías de información y comunicación, de manera que el acceso a la información oportuna y confiable, facilite el ejercicio efectivo de los derechos constitucionales y legales y los controles ciudadano, político, fiscal, disciplinario y de gestión o administrativo.

La Comisión Distrital de Sistemas de Bogotá D.C., en su calidad de organismo rector de las políticas y estrategias a nivel de tecnologías de la información y de las comunicaciones en el Distrito y órganos de control del Distrito Capital, mediante Resolución 305 de 2008 determinó el marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información, los procedimientos para el adecuado uso y administración de los recursos informáticos y señaló que el del Sistema de Gestión de Seguridad de la Información debe estar alineado con el Sistema Integrado de Gestión, en cada uno de sus componentes, esto es, los Sistemas de Gestión de Calidad, Control Interno, Desarrollo Administrativo y Gestión Ambiental.

El Gobierno Nacional, a través del documento CONPES 3701 del 14 de julio de 2011, estableció la Estrategia Nacional de Ciberseguridad y Ciberdefensa, con el fin de desarrollar medidas que

aseguren la información de los ciudadanos frente a las amenazas informáticas y que deben ser adoptados. De igual forma, a través el Documento CONPES 3854 se definió la Política Nacional de Seguridad Digital, cuyo objetivo era fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital. En el año 2020 nuevamente se impulsa el tema, mediante la creación del Documento CONPES 3995 DE 2020 que define la Política de Confianza y Seguridad Digital con el fin de establecer medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital.

El Decreto único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones N°1078 de 2015, dispone que las entidades que conforman la administración pública serán sujetos obligados al cumplimiento de las políticas y los lineamientos de la Política de Gobierno Digital establece que la Seguridad de la Información es uno de los habilitadores transversales, es decir, que es uno de los elementos fundamentales que permiten el desarrollo del Gobierno Digital y que busca preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

El Decreto Nacional 1499 de 2017, modificó el Decreto Único Reglamentario del Sector Función Pública 1083 de 2015, en su artículo 2.2.22.3.8 dispone que “cada una de las entidades integrará un Comité Institucional de Gestión y Desempeño encargado de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG, el cual sustituirá los demás comités que tengan relación con el Modelo y que no sean obligatorios por mandato legal”.

La Resolución 857 del 01 abril de 2019 resolvió la creación del Comité Institucional de Gestión y Desempeño y su naturaleza.

La Resolución 1395 del 23 agosto de 2019 en su Artículo 5 definió la creación del Equipo Técnico, en el marco de la Política de Seguridad Digital a cargo de la Oficina Administrativa de Redp y dentro de sus funciones está elaborar la documentación necesaria y solicitada, para el desarrollo de los temas técnicos a cada uno de los equipos técnicos.

La Resolución 1772 del 05 noviembre 2020 de la Secretaría de Educación del Distrito resuelve modificar el numeral 7 de la Resolución 857 de 2019, el cual quedará así:

> # 7. Las Políticas de Gestión y Desempeño Institucional en la Secretaría de Educación del Distrito, serán lideradas por las siguientes dependencias, sin detrimento de la participación de las demás involucradas en la implementación de cada uno de los requerimientos, teniendo en cuenta los numerales anteriores, del presente artículo, así:

Dimensiones	Políticas de Gestión y Desempeño Institucional	Dependencia Líder de la Implementación de la Política
Talento Humano	Gestión Estratégica Del Talento Humano	Dirección de Talento Humano
	Integridad	Dirección de Talento Humano
Direccionamiento Estratégico y Planeación	Planeación Institucional	Oficina Asesora de Planeación
	Gestión Presupuestal y Eficiencia del Gasto Público	Dirección Financiera
Gestión con Valores para Resultados	Fortalecimiento Organizacional y Simplificación de Procesos	Oficina Asesora de Planeación
	Gobierno Digital	Oficina Administrativa de RedP
	Seguridad Digital	Oficina Administrativa de RedP
	Defensa Jurídica	Oficina Asesora Jurídica
	Mejora Normativa	Oficina Asesora Jurídica
	Servicio al Ciudadano	Oficina de Servicio al Ciudadano
	Racionalización de Trámites	Oficina de Servicio al Ciudadano
	Participación Ciudadana en la Gestión Pública	Dirección de Participación y Relaciones Interinstitucionales
	Gestión Ambiental (Componente)	Oficina Asesora de Planeación
Evaluación de Resultados	Seguimiento y Evaluación del Desempeño Institucional	Oficina Asesora de Planeación
Información y Comunicación	Gestión Documental	Dirección de Servicios Administrativos
	Transparencia, Acceso a la Información Pública y Lucha Contra la Corrupción	Oficina Asesora de Planeación
	Gestión de la Información Estadística	Oficina Asesora de Planeación
Gestión del Conocimiento y la Innovación	Gestión del Conocimiento y la Innovación	Oficina Asesora de Planeación
Control Interno	Control Interno	Conjunta entre la Oficina Asesora de Planeación y la Oficina de Control Interno, de acuerdo con los roles y responsabilidades establecidos para la implementación de la política.

8. REVISIÓN

El Manual de la Política General de Gestión de Seguridad de la Información será periódicamente, con el fin de garantizar la pertinencia, oportunidad y vigencia. Esta actividad será adelantada por el equipo técnico de Seguridad Digital y deberá ser aprobado por el Jefe de la Oficina Administrativa de Redp de la Secretaria de Educación del Distrito.

9. ROLES Y RESPONSABILIDADES DEL EQUIPO TECNICO DE SEGURIDAD DIGITAL

De acuerdo a las indicaciones de la Resolución 1395 de 2019, además de las establecidas en el artículo 20 de la Resolución 857 de 2019, el equipo técnico en el marco de la política de Seguridad Digital cumplirá las siguientes funciones:

Prestar soporte técnico y recomendar la ejecución de iniciativas, proyectos y lineamientos sobre seguridad de la información, en especial el Plan de Tratamiento de Riesgos, según lineamientos del MinTic y DAFP. Así como, velar por la adopción de los controles y ser el facilitador para el seguimiento de los indicadores en el cumplimiento del SGSI.

Realizar el diagnóstico del estado de la seguridad de la información de la Secretaría de Educación del Distrito.

Realizar y analizar los consolidados de información sobre los incidentes de seguridad presentados.

Establecer y proponer el Plan de Tratamiento de Riesgos para la SED.

Generar las alertas preventivas y proponer los ajustes a la política de seguridad que garanticen la reducción de la exposición al riesgo de los Activos de información.

Recomendar el uso de metodologías, herramientas y procedimientos específicos para la seguridad de la información según el DAFP.

Proponer las estrategias para la divulgación y comunicación de las políticas y normas de seguridad que la Secretaría de Educación del Distrito expida.

Identificar los ajustes requeridos a los procesos y procedimientos y proponer herramientas informáticas de punta que eliminen o mitiguen los riesgos.

Establecer contacto con las autoridades pertinentes, grupos de interés especial, foros y asociaciones profesionales especializadas en seguridad.

Realizar el respectivo seguimiento al grado de avance de la implementación de las políticas de Gobierno Digital y Seguridad Digital y formular las acciones de mejora que permitan optimizar la eficacia, eficiencia y efectividad de las mismas.

Elaborar la documentación necesaria y solicitada, para el desarrollo de los temas técnicos a cada uno de los equipos técnicos.

Desarrollar acciones de promoción, divulgación, sensibilización y/o capacitación de las herramientas, instrumentos y/o lineamientos que apoyan la implementación de las políticas de la gestión y desempeño institucional a su cargo.
Presentar los informes que le sean requeridos, por el Comité Institucional de gestión y desempeño o cualquier otra instancia interna o externa, sobre los asuntos a su cargo.

Definiciones

- **Propietario de la información**

Es la unidad organizacional o área en donde se origina la información, y el responsable por el activo de información. La persona designada como ***Propietario*** de la información tiene las siguientes responsabilidades:

- Mantener actualizado el inventario de los activos de información de los procesos a su cargo.
- Determinar el nivel de clasificación de cada uno de los activos de información de los cuales es responsable, de acuerdo con su impacto para el negocio y sus objetivos estratégicos.
- Propender por el cumplimiento de la política de seguridad de la información para establecer y velar porque se mantenga la confidencialidad, la integridad y la disponibilidad de los activos de información a su cargo.
- Identificar y analizar los riesgos a los cuales se encuentran expuestos los activos de información a su cargo.
- Definir los controles necesarios para los activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido.
- Validar la operación de los controles definidos.
- Aprobar el acceso de funcionarios y terceros a los activos de información de los procesos a su cargo, para que este se realice únicamente cuando sea necesario.
- Monitorear los niveles de acceso de funcionarios y terceros a los activos de información de los procesos a su cargo, para validar la confidencialidad e integridad de la información almacenada, resguardada o procesada en los mismos.
- Comunicar los riesgos, incidentes y necesidades al equipo técnico de Seguridad Digital de manera oportuna, e implementar las medidas o acciones recomendadas.

- **Custodio de la información**

Es la unidad, proceso o área responsable de la administración y monitoreo de la seguridad en los activos de información (información física, equipos, software, sistemas de Información, accesorios, entre otros).

El custodio de la Información tiene las siguientes responsabilidades:

- Implementar y mantener los requerimientos de seguridad de la información especificados por el "*PROPIETARIO"* de la Información.
- Proporcionar asistencia al "*PROPIETARIO"* de la Información en la selección de soluciones técnicas apropiadas.
- Realizar monitoreo permanente de la seguridad de la información de los activos de información a su cargo, para validar la confidencialidad e integridad de la información almacenada, resguardada o procesada en los mismos.
- Identificar y analizar los riesgos a los cuales se encuentran expuestos los activos de información a su cargo.
- Definir los controles necesarios para los activos de información de acuerdo con los niveles de clasificación establecidos y el nivel de seguridad requerido.
- Validar la operación de los controles definidos.

- Definir los procesos correspondientes de su área para garantizar el cumplimiento de los criterios de seguridad de la información.
- Mantener registros permanentes y salvaguardar los históricos para facilitar la trazabilidad de los activos de información y el acceso a los mismos.

- **Usuario final**

Es aquella persona que utiliza la información. El usuario final tiene las siguientes responsabilidades:

- Conocer, acatar y aplicar las políticas y procedimientos apropiados.
- Conocer, acatar y aplicar las políticas de seguridad de la información y los procedimientos apropiados con relación al manejo de la información y de los sistemas informáticos y los controles técnicos de seguridad de la información de la Entidad.
- Mantener la confidencialidad e integridad de los activos de información provistos por la Entidad para llevar a cabo sus labores.
- No permitir y no facilitar el uso de los sistemas informáticos a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software, datos y otros) y de telecomunicaciones (teléfono, fax y otros) para otras actividades que no estén directamente relacionadas con los objetivos misionales de la Secretaría de Educación del Distrito.
- Proteger meticulosamente sus datos de acceso a los sistemas de información.
- Reportar inmediatamente al jefe inmediato o al Equipo Técnico de Seguridad Digital, de cualquier evento que pueda comprometer la seguridad de la Institucióny sus recursos informáticos.
- Acatar y seguir los procedimientos definidos en el cumplimiento de la seguridad de la información.

- **Oficina de Control Interno y Oficina de Control Disciplinario**

El equipo técnico de Seguridad Digital notificará a las oficinas de Control Interno y Oficina de Control Disciplinario,las situaciones detectadas que por el incumplimiento de la política de seguridad de la información y normatividad aplicable, impliquen dar traslado a éstas instancias para su respectivo trámite y actuación en concordancia con la normatividad vigente.

- **Grupo funcional de apoyo en la atención de incidentes de seguridad de la información de la Oficina Administraba de RedP**

En la SED se cuenta con personal calificado técnicamente para realizar la atención a requerimientos, auditoría, seguimiento y atención a incidentes de Seguridad de la información.

También este personal realizará actividades de seguridad informática en los siguientes procesos:

a. Conceptos y certificación de seguridad de productos y proyectos.
b. Recolección de información y estadísticas (indicadores) de activos de información dedicados a la seguridad.
c. Informática forense.
d. Proceso de sensibilización, capacitación y alertas de seguridad

e. Gestión de solicitudes, quejas e incidentes de seguridad.
f. Gestión de correlación de eventos y monitoreo (preventivo y correctivo).
g. Planeación y ejecución de auditorías de seguridad de la información.
h. Generar los informes y seguimiento a los indicadores de eficiencia y eficacia de los controlesy del SGSI.

Las actividades de planificación, definición de procesos, el seguimiento y ajuste a la seguridad informática de cada uno de los activos de información de la SED son de responsabilidad de los dueños (Propietarios) y de los custodios de la información y deben cumplir las políticas generales y específicas de cada uno de estos.

10. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

El equipo técnico de Seguridad Digital se alinea con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la estrategia de Gobierno Digital como son TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Los procedimientos están basados en las declaraciones de los dominios del sistema de gestión de seguridad de la información de la ISO 27001:2013 y del modelo MSPI de MinTic. El conjunto de dominios y controles se implementan como procedimientos al interior de la SED y constituyen la base sólida para generar la documentación de procesos y procedimientos de la seguridad de los activos de información.

11 DECLARACION DE LOS DOMINIOS DE LA POLITICA DE SEGURIDAD DE LA INFORMACIÓN

11.1.1 Organización de la seguridad de la información

La Secretaría de Educación del Distrito, establece el marco de referencia de gestión, implementación y operación de la política general de gestión de seguridad de la información, para lo cual define los roles, responsabilidades, de las personas, áreas y comités con el fin de reducir el riesgo de modificación no autorizada, no intencional o el uso indebido de los activos de información de la entidad.

11.1.2 Seguridad de los recursos humanos

La Secretaría de Educación del Distrito propende porque los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general, todas las personas entiendan sus responsabilidades frente a la seguridad de la información y estén debidamente informados y capacitados para que las funciones que desarrollen reduzcan el riesgo de robo, fraude, mal uso de las instalaciones y medios, y así asegurar la confidencialidad, disponibilidad e integridad de la información;

Para esto la entidad desarrolla estrategias de comunicación y capacitación para sensibilizar sobre los riesgos y vulnerabilidades y vela porque en los acuerdos contractuales con los servidores públicos y contratistas se establezcan responsabilidades y compromisos.

La Secretaría define un proceso formal y comunicado para el emprendimiento de acciones contra servidores públicos y contratistas que hayan cometido una violación a la seguridad de la información.

11.1.3 Gestión de activos de información

La Secretaría de Educación del Distrito establece una metodología para la gestión de riesgos, actualiza el inventario de activos de información y establece procedimientos claros para los servidores públicos, contratistas o terceros para la entrega y devolución de los activos de información, al inicio o terminación de su actividad.

La entidad define controles pertinentes para la gestión de medios de soporte removibles y fijos digitales, la disposición final de los mismos en forma segura y la protección contra acceso no autorizado, uso indebido o corrupción durante la transferencia.

11.1.4 Control de acceso

La Secretaría de Educación del Distrito a través de los **propietarios** de los activos de información implementa las políticas y procedimientos para el control de acceso a los activos de información y a las instalaciones de procesamiento de información o almacenamiento físico. Igualmente, norma, regula y registra el acceso a redes de comunicaciones y sus servicios y el acceso autorizado a información privilegiada.

La Entidad propende porque la autenticación de los usuarios se realice de manera secreta, que se cumplan los criterios para el manejo de contraseñas y se implementen conexiones “seguras”.

Se restringe y controla el uso de programas que podrían tener capacidad de anular, bloquear o interceptar la información de los sistemas y controlar el acceso a los códigos fuente de los programas.

11.1.5 Cifrado (criptografía)

La Secretaría de Educación del Distrito está comprometida con el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información y establece requisitos sobre el uso de controles criptográficos y gestión de claves.

11.1.6 Seguridad física y ambiental

La Secretaría de Educación del Distrito propende por la protección de las instalaciones físicas de la entidad con el fin de prevenir el acceso no autorizado, daño o interferencia en los activos de información. Para esto estable los siguientes lineamientos:

Disponer de los recursos y acciones necesarias para ubicar en sitios seguros y protegidos los equipos y elementos que permitan reducir los riesgos de amenazas, peligros ambientales y las posibilidades de acceso no autorizado. Igualmente dotará los elementos necesarios para proteger la infraestructura de amenazas y de incidentes ocasionados por fallas en la potencia y otras interrupciones causadas por servicios públicos.

El cableado de potencia y de telecomunicaciones que soporta los datos y brinda soporte a los servicios de información, son protegidos contra interceptaciones, interferencia o daño y se define un plan de mantenimiento adecuado para asegurar su disponibilidad e integridad

Se aplican medidas de seguridad a los activos que se encuentran fuera de los predios de la Secretaría de educación del Distrito, teniendo en cuenta los diferentes riesgos de trabajar fuera de

dichos predios, tales como dispositivos móviles o equipos o sistemas en tercerización en modalidad de servicio (SaaS, IaaS, hosting, colocación, entre otras).

La entidad hace disposición final segura y controla la reutilización de equipos, verificando que todos los elementos que contengan medios de almacenamiento sean retirados o borrados y según el caso destruidos, para asegurar que cualquier dato confidencial o software con licencia no sea expuesto a un riesgo de seguridad.

La Secretaría de Educación del Distrito realiza controles y campañas de sensibilización para asegurar que los equipos se mantengan con la supervisión y la protección apropiada y adopta las prácticas de **"escritorio limpio**" para los papeles y medios de almacenamiento removibles.

11.1.7 Seguridad operativa y ambiental

La Secretaría de educación del Distrito define, controla, documenta los procesos, procedimientos y manuales operativos para ponerlos a disposición de todos los usuarios. Se controlan los cambios en la entidad de los procesos, instalaciones y la infraestructura tecnológica y se previene que dichos cambios pongan en riesgo la seguridad de la información.

La Entidad separa los ambientes de desarrollo, pruebas y producción, para reducir los riesgos de acceso indebido o cambios no autorizados al ambiente operacional. Define e implementa los controles de detección, prevención y recuperación de datos y sistemas.

La entidad implementa y documenta procesos eficaces, eficientes y controlados para la gestión de las copias de respaldo de la información, software e imágenes de los sistemas y pone a prueba regularmente la capacidad de recuperación.

En la Secretaría de Educación del Distrito se registran, elaboran, conservan y revisan los registros (protegidos contra alteración y acceso no autorizado) de las actividades de los usuarios, las fallas, incidentes y eventos que se han materializado y han puesto en riesgo la seguridad de la información.

En la Secretaría de Educación del Distrito las actividades de los administradores técnicos y funcionales, de los operadores delos diferentes sistemas de información, bases de datos, sistemas operativos y demás, se registran, protegen y se revisan con regularidad. Igualmente, la entidad mantiene sincronizado los relojes de todos los sistemas de procesamiento de información pertinentes con una única fuente de referenciade tiempo.

La entidad implementa procedimientos para controlar la instalación de software en sistemas operativos, obtiene información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

La Secretaría de Educación del Distrito establece e implementa las mejores prácticas de seguridad para la instalación de software por parte del usuario y establece políticas sobre la auditoría y gobernabilidad de las tecnologías de información.

11.1.8 Seguridad en las telecomunicaciones

La Secretaría de Educación del Distrito adopta los procesos y establece las acciones necesarias para garantizar la disponibilidad y seguridad en las redes de comunicaciones y a los procesos de transferencia de información internos o con terceros.

Establece el acuerdo de nivel de servicios de la red de comunicaciones interna y externa, toma acciones de separación física y lógica de las redes en grupos de servicios de información, usuarios y sistemas de información y establece las acciones para proteger los mensajes electrónicos.

La entidad identifica, revisa regularmente y documenta los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la SED y la ley.

11.1.9 Adquisición, desarrollo y mantenimiento de los sistemas de información

La Secretaría de Educación del Distrito documenta y define los requisitos de seguridad que deben cumplir todos los sistemas de información. Esto incluye los requisitos para sistemas de información, programas, software, aplicativos tanto para uso interno o dispuestos para terceros o a la comunidad educativa.

La Secretaría de Educación del Distrito define los requisitos relacionados con seguridad de la información para las mejoras a los sistemas de información existente y establece normas y procedimientos para las aplicaciones enlínea y portales en las redes públicas para evitar actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.

La entidad protege la información de las transacciones de servicios de aplicaciones para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.

La Secretaría vela porque la política de seguridad esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información, estableciendo y aplicando reglas para el desarrollo de software o adquisición de sistemas de información internos o tercerizados. Igualmente vela porque se gestione y controlen los cambios y las prueba para asegurar que no haya impacto adverso en las operaciones o seguridad.

11.1.10 Relaciones con los proveedores.

La Secretaría de Educación del Distrito define, documenta, hace seguimiento, revisa y audita los activos de información que son accesibles a los proveedores.

La entidad establece y acuerda todos los requisitos de seguridad de la información pertinentes con cada proveedor en el acceso, procesamiento, almacenamiento, comunicación o suministro de componentes de infraestructura de TI para la información de la organización.

La Secretaría de Educación del Distrito controla los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos

11.1.11 Gestión de incidentes en la seguridad de la información

La Secretaría de Educación del Distrito promueve a que los empleados y contratistas, que usan los servicios y sistemas de información, informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios. Igualmente define y comunica el procedimiento para la gestión de incidentes que permita contrarrestar de forma oportuna, las interrupciones generadas por eventos, fallas o desastres.

La Secretaría de Educación del Distrito establece las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información y los mecanismos de información a través de los canales de gestión apropiados.

La secretaría de Educación del Distrito evalúa, clasifica, y documenta los incidentes de seguridad de la información y da respuesta a los mismos. Igualmente sistematiza el conocimiento adquirido en la resolución de incidentes para reducir la posibilidad o el impacto de incidentes futuros.

La entidad define y aplica procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

11.1.12 Aspectos de seguridad de la información en la gestión de la continuidad del negocio

La Secretaría de Educación del Distrito establece, documenta, implementa y mantiene los procesos, procedimientos y controles para planes de continuidad y determina sus requisitos para la seguridad de la información en situaciones adversas (crisis o desastres).
Igualmente verifica a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que sean válidos y eficaces durante situaciones adversas.

Finalmente, la Secretaría de Educación del Distrito dispone las instalaciones de procesamiento de información con redundancia suficiente para cumplir los requisitos de disponibilidad.

11.1.13 Cumplimiento

La Secretaría de Educación del Distrito vela por la identificación, documentación, actualización y cumplimiento de los requisitos legales vigentes enmarcados en la seguridad de la información con el fin de evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y propende porque se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.

La entidad implementa procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.

La entidad asegura la privacidad y la protección de la información personal, como se exige en la legislación y la reglamentación pertinentes.

La Secretaría de Educación del Distrito establece criterios para la revisión de los objetivos de control, los controles, la política,los procesos y los procedimientos para seguridad de la información por entidades externas a intervalos planificados o cuando ocurran cambios significativos.

La Secretaría de Educación del Distrito establece que el personal de alta dirección (secretaria, subsecretarios, directores, jefes entre otros) revise con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.

11. INVENTARIO DE ACTIVOS DE INFORMACIÓN

La SED ha definido utilizar la metodología de gestión de activos de información de acuerdo a la Política de Gestión documental definida en la 5ª dimensión “Información y comunicación” de MIPG, para la gestión del inventario de activos de información exacto, actualizado y consistente para permitir definir la criticidad, los propietarios, custodios y los usuarios de los mismos.

Igualmente, la documentación generada en la Entidad deberá seguir los lineamientos de la política de gestión documental.

12. IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS.

La SED usará la Metodología de Administración de riesgos para identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos los activos, así como la declaración de aplicabilidad, empleando los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad.

13. PLAN DE COMUNICACIONES

La SED define el Plan de comunicación, sensibilización y capacitación para la adopción de la cultura de la seguridad de la información y generar competencias y hábitos en todos los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general a todas las personasque usen la información de la entidad.

Este plan es ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad y el apoyo de la Oficina Asesora de Planeación, Oficina Administrativa de Redp, Oficina Asesora de Comunicación y Prensa y la Dirección de Talento Humano.

Para el efecto, se utilizarán los siguientes medios:

Publicación Red académica de instructivos de Seguridad de la información para servidores públicos y contratista de la Sed.
Memorando interno
Intranet
Talleres
Mensajes de sensibilización en medios electrónicos internos

La Política de Seguridad contenida en este documento deberá ser conocida y cumplida por todos los servidores públicos, contratistas, terceros, aprendices, practicantes, usuarios y en general todas

las personas que haga uso de los activos de información de la Secretaría de Educación del Distrito. El incumplimiento de la misma se considerará un incidente de seguridad.

14. MEJORA CONTINUA Y APROBACION DEL MANUAL DE LA POLITICA

El equipo técnico de Seguridad Digital será el encargado de proponer mejoras al Manual de la política basado en el monitoreo a los indicadores de cumplimiento que se expresan en el presente manual, y da el aval para su aprobación por parte del líder de la Política de Seguridad Digital.

15. VIGENCIA

La versión oficial de este documento será la que se encuentre publicada y aprobada en el Manual de Procesos y Procedimientos de la Secretaría de Educación del Distrito.

16. CONTRAVENCIONES

Las infracciones a la Política de Seguridad de la información en la Secretaría de Educación del Distrito serán informadas a las instancias correspondientes para que se definan las Acciones Administrativas, Acciones disciplinarias y Acciones penales según el caso.

17. INDICADOR DE CUMPLIMIENTO

Nombre Indicador	**Tipo Indicador**	**Objetivo del Indicador**	**Variables del Indicador**
Implementación de la Política de Seguridad de la Información adoptada por la Entidad.	Eficacia	Mide el avance por parte de la Entidad de la aplicación de la Política de Seguridad de la Información.	Porcentaje: Acciones implementadas en la lista de controles sobre las acciones definidas.

Nombre Indicador	**Tipo Indicador**	**Objetivo del Indicador**	**Variables del Indicador**
Actividades de sensibilización	Eficacia	Mide el avance de la campaña de comunicación y sensibilización	Porcentaje: Actividades de sensibilización realizadas sobre las actividades planteadas

Nombre Indicador	Tipo Indicador	Objetivo del Indicador	Variables del Indicador
Inversión anual en el desarrollo de la política de seguridad de la información	Eficiencia	Mide la inversión anual dedicada a las acciones de seguridad de la información.	Crecimiento de la inversión en SGSI por año, discriminado por concepto.

Anexo 1 GLOSARIO DE TERMINOS

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 para la Secretaría de Educación del Distrito.

Alta Dirección: Se considera a los directivos con el cargo más alto en la Secretaría de Educación del Distrito. (En principio, el Secretario, Subsecretarios y Jefes de Oficinas Asesoras).

Análisis de riesgos: Uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Área Crítica: Es el área física donde se encuentran instalados los equipos de cómputo y telecomunicaciones que requieren de cuidados especiales y son indispensables para el funcionamiento continuo de los sistemas de comunicación de los centros de datos.

Auditoría: Es el proceso de llevar a cabo una inspección y/o un examen independiente de los registros del sistema y actividades para probar la eficiencia de la seguridad de datos y procedimientos de integridad de datos, para asegurar el cumplimiento de la política establecida y recomendar cualquier cambio que se estime necesario.

Backup o copia de seguridad: Copia de respaldo de la información.

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.

Criticidad: Medida del impacto que tendría la Organización debido a una falla de un sistema y que éste no funcione como es requerido.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Equipo de Telecomunicaciones. Todo dispositivo capaz de transmitir y/o recibir señales digitales o analógicas para comunicación de voz, datos y video, ya sea individualmente o de forma conjunta.

Evento de Seguridad de la Información: Se considera un Evento de Seguridad de la Informacióna cualquier situación identificada que indique una posible brecha en las Políticas de Seguridad o fallaen los controles y/o protecciones establecidas.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Incidente de Seguridad de la Información: Se considera un Incidente de Seguridad de la Información a cualquier evento que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencias, el número de veces ocurrido o el origen (interno o externo).

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Instructivo: Documento que describe de una manera detallada cómo debe ejecutarse una actividad o tarea determinada para garantizar su realización, hablan sobre métodos específicos sobre plataformas, sistemas de información o algún proceso definido.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

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.

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 del a dependencia donde ellos se aplican.

Segregación de Funciones (tareas): La segregación de funciones o de tareas está orientada a evitar que una misma persona tenga accesos a dos o más responsabilidades dentro del sistema, de tal forma que pueda realizar acciones o transacciones que lleven a la consumación de un fraude.

Seguridad de la información: se entiende como la preservación de las siguientes características:

- Confidencialidad: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
- No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
- Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que esté sujeta la Secretaría de Educación del Distrito.
- Confiabilidad de la Información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

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.

Soportes físicos: Datos en soporte papel (cartas, informes, normas, contratos) o en medios de almacenamiento físico.

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Elaboró	Revisó	Aprobó
Edgar Fernando Ortega Galán Profesional Especializado OAP 15 febrero 2022	Henry Moyán Contratista OARedp Luis Sarmiento Contratista OARedp Julio Andrés Sánchez Contratista OARedp 15 febrero 2022	Wilson Adiel Rodríguez Jefe OAredp 15 febrero 2022