Política General de Seguridad de la Información

1 Objetivo

Establecer directrices, lineamientos, condiciones, pautas y establecimiento de controles necesarios para la protección de la información en el Ministerio de Educación Nacional-MEN, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información.

1.1 Objetivos Específicos

1.1.1 Establecer, implementar controles lógicos y físicos, lineamientos en materia de seguridad de la información.
1.1.2 Fortalecer la cultura en seguridad de la información en los colaboradores y terceros del MEN.
1.1.3 Reducir el impacto de los riesgos de seguridad de la información con controles adecuados de acuerdo con la misión y visión del Ministerio de Educación Nacional.

2 Alcance

Las presente Política aplica para todos los colaboradores y terceros del MEN que tengan acceso a la información institucional. Las directrices, responsables y soportes detallados se encuentran establecidos en la matriz de aplicabilidad y demás documentación complementaria establecida por el Sistema de Gestión de Seguridad de la Información del Ministerio la cual cumple con la normativa vigente y se encuentra acorde con lo definido por los estándares y buenas prácticas de seguridad de la información.

3 Aplicabilidad

Las presente Política sus objetivos, además de los manuales, procedimientos o documentos derivados o complementarios aplican a todos los colaboradores y terceros del MEN, así como aquellas personas que en razón del cumplimiento de sus funciones y las del Ministerio, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información.

El incumplimiento a la Política de Seguridad y Privacidad de la Información o de sus lineamientos derivados, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad

4 Definiciones

- **Acceso Lógico:** restricción de acceso a los datos. Esto se logra mediante técnicas de ciberseguridad como id.
- **Activo de Información:** es todo aquello que en el MEN es considerado importante o de alta validez para el mismo, porque contiene información importante, como son los datos creados o utilizados por procesos de la organización, en medio digital, en papel o en otros medios. Ejemplos: bases de datos con usuarios, contraseñas, números de cuentas, informes etc.
- **Alta Dirección:** persona o grupo de personas que dirigen y controlan al más alto nivel una entidad. Es la máxima autoridad en el sistema.
- **Amenaza:** es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en un equipo, como por ejemplo un virus.
- **Carpeta Compartida:** carpeta cuyo contenido es accesible por todos los usuarios que pertenecen a un mismo grupo de trabajo.
- **Ciberseguridad:** es el proceso de proteger los activos de información por medio del tratamiento de las amenazas a la información que es procesada, almacenada y/o transportada a través de sistemas de información interconectados.
- **Confidencialidad:** propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.
- **Controles:** medida que permite reducir o mitigar un riesgo.
- **Copias de respaldo:** copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida. Suele conservarse en un lugar seguro, generalmente en un dispositivo distinto de aquel en el que se encuentra el original y lejos de este. De esta forma, si la información original se daña es posible reconstruirla a partir de la copia.
- **Dato:** es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **Disponibilidad:** propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Grupos de Valor**: son las personas naturales (o jurídicas (organizaciones públicas o privadas), grupos étnicos (indígenas y ROM) a quienes van dirigidos los bienes y servicios de una entidad. Es importante que la entidad tenga identificado a sus grupos de valor por rasgos como su ubicación, condiciones económicas, sociales, culturales, entre otros.
- **Grupos de Interés**: son los individuos u organismos específicos que tienen un interés especial en la gestión y los resultados de la entidad, como gremios, asociaciones de usuarios (agricultores, transportadores), sindicatos, universidades, entre otros.

- **Integridad:** propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Información:** conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **MEN:** Ministerio de Educación Nacional.
- **MSPI:** modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MINTIC.
- **OTSI:** Oficina de Tecnología y Sistemas de Información del MEN
- **Sistema de Gestión de Seguridad de la Información:** es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Riesgo:** posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Vulnerabilidad:** es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

5 Compromiso de la Alta Dirección

La Alta Dirección del Ministerio de Educación Nacional – MEN se compromete a liderar y respaldar el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI. Así mismo, revisará de manera periódica los avances en su implementación y garantizará la disponibilidad de recursos suficientes, tanto tecnológicos como de talento humano calificado, para asegurar su funcionamiento. De igual forma, la seguridad de la información será considerada dentro de las decisiones estratégicas de la entidad.

6 Roles y responsabilidades

El MEN, define los roles y responsabilidades para la implementación del MSPI y el cumplimiento de los lineamientos de seguridad descritos en esta política y los demás documentos derivados del SGSI, de acuerdo con la siguiente clasificación:

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Alta Dirección	• Proporcionar los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información-SGSI (Recursos económicos, formación y recursos tecnológicos).
Comité de Gestión y Desempeño o quien haga sus veces	• Aprobar los recursos correspondientes para la implementación y el mantenimiento del sistema de gestión de seguridad de la información-SGSI.
OTSI	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información.
Oficial de Seguridad de la información	• Analizar, definir, documentar y gestionar el plan estratégico de seguridad de la información, proponiendo las decisiones necesarias para su adecuada gestión, en concordancia con la política y los lineamientos definidos y aprobados por la entidad. • Coordinar las actividades relacionadas con el diseño, implementación, operación, revisión y mejora continua del Sistema de Gestión de Seguridad de la Información, articulando su desarrollo con todos los procesos de la entidad. • Apoyar a la Oficina de Tecnologías y Sistemas de la Información – OTSI en la identificación, selección e implementación de mecanismos, controles y herramientas tecnológicas necesarias para el tratamiento de los riesgos de seguridad de la información. • Contribuir a la elaboración de lineamientos (manuales, procedimientos y formatos) que fortalezcan el establecimiento y la mejora continua del Sistema de Gestión de Seguridad de la Información en la entidad. • Asegurar que los colaboradores tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos.

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Subdirección Talento Humano	• Incluir dentro del Plan Institucional de Capacitación-PIC, capacitación y formación en materia de seguridad de la información. • Incluir en la agenda de las jornadas de inducción y reinducción temas de seguridad de la información, en coordinación con la OTSI, con el fin de fortalecer el conocimiento en este ámbito entre los funcionarios.
Oficina de Control Interno	• Incluir la seguridad de la información dentro del plan anual de auditoría institucional, desde el enfoque basado en riesgos. • Verificar el cumplimiento de la política, objetivos y controles establecidos en el Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con lo definido en los estándares y buenas prácticas a nivel de seguridad de la información. • Evaluar periódicamente la eficacia de los controles implementados y documentarlos por medio de informes de auditoría o seguimiento, de acuerdo con lo establecido en los planes de mejoramiento institucionales. • En caso de que se identifique una posible vulnerabilidad que afecte la integridad de los sistemas de información se informará a la alta Dirección mediante del Comité Institucional de Coordinación de Control Interno. • Realizar seguimiento a la implementación de planes de mejoramiento derivados de auditorías o hallazgos en materia de seguridad de la información. • Promover la cultura de autocontrol y cumplimiento de lineamientos de seguridad de la información en la entidad, en concordancia a las estrategias definidas de uso y apropiación lideradas por la OTSI.
Oficina Asesora de Comunicaciones	• Apoyar en la ejecución de acciones de comunicación y sensibilización en seguridad de la información, garantizando su difusión en todos los niveles de la entidad

ROL / INSTANCIA / DEPENDENCIA	RESPONSABILIDADES
Subdirección de Contratación	• Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad. • Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en procesos o contratos.
Subdirección de Relacionamiento con la Ciudadanía	• Liderar e implementar controles de seguridad para la información física que gestiona y mantiene el Ministerio de conformidad con el plan de conservación documental. • Apoyar las estrategias de etiquetado de la información con el fin de realizar un proceso de clasificación más eficiente. • Apoyar en los procesos de articulación entre las tablas de retención documental y la identificación, clasificación y aceptación de activos de información de cada uno de los procesos del MEN. • Apoyar los procesos de interoperabilidad del SGDEA con los diferentes sistemas de información que generan documentos que de conformidad con las tablas de retención documental deben ser conservados totalmente.
Líderes de Proceso	• Implementar las políticas y procedimientos de seguridad de la información que se definan como parte del SGSI (Por ejemplo: gestión de activos, gestión de riesgos, entre otros).
Colaboradores (funcionarios y contratistas) y terceros	• Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos. • Cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados.

7 Principios

La presente política se fundamenta en los siguientes principios:

1. La información es uno de los activos más importantes del Ministerio y por lo tanto se espera que sea utilizada acorde con los requerimientos de sus funciones.
2. La Confidencialidad de la información del Ministerio y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y que sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones u obligaciones.
3. La Disponibilidad de la información en el Ministerio debe garantizarse de forma permanente cuando sea requerida.

8 Declaraciones

La Oficina de Tecnologías y Sistemas de Información-OTSI, motiva a colaboradores y terceros del MEN, cumplir con la política y demás documentación asociada con el SGSI, con el fin de proteger la información producida, recibida, recolectada almacenada o transferida. Para esto, se definen las siguientes premisas de seguridad de la información:

1. Las responsabilidades frente a la seguridad de la información serán definidas, socializadas, publicadas por parte de la OTSI y serán aceptadas por cada uno de los colaboradores y proveedores que tengan acceso a la información institucional
2. El MEN es responsable de los activos de información; sin embargo, los propietarios de dichos activos serán los colaboradores autorizados y encargados de la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, así como del hardware o la infraestructura tecnológica. Estos colaboradores deberán implementar los controles necesarios para su protección, de acuerdo con la clasificación de la información bajo su custodia. Los colaboradores y terceros deben cumplir los lineamientos e instrucciones descritos en esta política y demás documentación publicada dentro del Sistema Integrado de Gestión, así como los conceptos y lineamientos en materia de seguridad de la Información generados a solicitud.
3. La información producida, recibida, recolectada, almacenada o transferida por el Ministerio cuenta con la protección y seguridad mediante la definición, implementación, seguimiento y mejoramiento de herramientas, controles, procedimientos, etc., con el fin de evitar los riesgos asociados a su confidencialidad, integridad, y disponibilidad.
4. Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento.

5. Con el fin de mitigar las vulnerabilidades y amenazas relacionadas con el recurso humano, la alta dirección destinará los recursos suficientes para el desarrollo de programas de capacitación y sensibilización; es obligación de los colaboradores asistir a estos eventos o cursos en materia de seguridad de la información.

6. Los colaboradores tienen la obligación y responsabilidad de la identificación y notificación de cualquier incidente o evento que pudiera comprometer la seguridad de sus activos de información. Asimismo, el Ministerio deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

7. Dentro del manual de seguridad de la información se establecen los roles y responsabilidades específicos, relacionados con el Sistema de Gestión de Seguridad de la Información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

8. Es responsabilidad de los colaboradores del MEN realizar copia de seguridad de los archivos producidos, gestionados o administrados que se encuentren almacenados en los equipos de cómputo asignados; esta copia debe almacenarse en los medios designados por el Ministerio tales como servidor de archivos, almacenamiento en la nube, entre otros. Una vez finalizada la vinculación con la Entidad se deberá entregar toda la información procesada, al jefe inmediato o al supervisor de contrato.

9. Los equipos de cómputo de propiedad de los contratistas deberán cumplir con características mínimas antes de ser conectados en las redes de datos del Ministerio, esto a nivel de seguridad (actualizaciones, antivirus, entre otros) y uso de software legal. En caso de presentarse algún incidente identificado con el equipo del contratista, la Entidad podrá iniciar las acciones legales y administrativas correspondientes.

10. Con el fin de desarrollar el marco de actuación adecuado para la protección de la información y dar a conocer los lineamientos específicos en materia de seguridad de la información, el Ministerio establece esta política como el documento principal junto con el Manual del Sistema de Seguridad de la Información.

11. Los proyectos o iniciativas que desarrolle el Ministerio que requieran del componente de tecnologías de la información relacionados con el desarrollo y/o adquisición de software o cualquier componente TIC deberá contar con el aval de la Oficina de Tecnologías y Sistemas de la Información.

9 Seguimiento, revisión y evaluación

El MEN a través de la OTSI realizará revisiones periódicas al SGSI. Dichas revisiones estarán enfocadas en los siguientes aspectos:

1. Revisión de indicadores definidos para el Sistema de Gestión de Seguridad de la Información.
2. Revisión de avance en la implementación del Modelo de Seguridad y Privacidad de la Información del Ministerio TIC.
3. Revisión de avance de la Política de Seguridad Digital de acuerdo con lo solicitado por FURAG o la herramienta definida para tal fin.
4. Periódica anual, donde se deberá revisar la efectividad de la política y sus objetivos.
5. Cambios estructurales en el Ministerio (restructuración de dependencias o procesos).
6. Incidentes de seguridad de la información que requieran cambios dentro de la política.

10 Sanciones

1. Cualquier violación a las políticas de seguridad de la información del Ministerio de Educación Nacional-MEN debe ser sancionada de acuerdo con el Reglamento Interno de Trabajo, a las normas, leyes y estatutos de la ley colombiana, así como la normativa atinente y supletoria, y apoyados en las leyes regulatorias de delitos informáticos de Colombia.
2. Las sanciones podrán variar dependiendo de la gravedad y consecuencias generadas de la falta cometida o de la intencionalidad de esta.

Control de Cambios		
Versión	**Fecha de vigencia**	**Naturaleza del cambio**
01	Rige a partir de su publicación en el SIG	Se crea la política para establecer las directrices, lineamientos, condiciones, pautas y establecimiento de controles necesarios para la protección de la información en el Ministerio de Educación Nacional-MEN.

Registro de aprobación					
Elaboró		**Revisó**			**Aprobó**
Nombre	Diego Ramirez Pulido	**Nombre**	Ana Yised Castro Ortiz	**Nombre**	Daniel Guillermo Torres Niño
Cargo	Contratista de la Oficina de Tecnología y Sistemas de Información	**Cargo**	Coordinadora del equipo de infraestructura Tecnológica	**Cargo**	Jefe de la Oficina de Tecnología y Sistemas de Información