ESCUELA CONTRA LA DROGADICCIÓN
Luis Carlos Galán Sarmiento UNIDOS

GOBERNACIÓN DE ANTIOQUIA

UNIDOS

POLITICA DE SEGURIDAD DIGITAL

Documento actualizado conforme a la versión 05 del Manual Operativo MIPG
Aprobada en Comité de Gestión y Desempeño el 25 de abril de 2023

FABIO VILLA RODRIGUEZ
Director General

TABLA DE CONTENIDO

INTRODUCCION

El Modelo Integrado de Gestión y Planeación -MIPG- es el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.[1]

El MIPG surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno, mediante el Decreto 1083 de 2015 (Decreto único del Sector Función Pública), modificado por el Decreto 1499 de 2017.

La competencia para **definir y actualizar** el MIPG le corresponde al Consejo para la Gestión y el Desempeño Institucional, órgano del más alto nivel del Estado Colombiano conformado por las "entidades líderes de política"; el Consejo para la Gestión y el Desempeño Institucional es la **única** instancia donde se decide los temas relacionados con las políticas de gestión y del desempeño institucional (proponer políticas, normas, herramientas, métodos y procedimientos en materia de gestión y desempeño institucional).

Por su parte, a las entidades públicas le corresponde la **Implementación** del MIPG, no tienen competencia para formular total ni parcialmente las políticas de gestión y desempeño.

La Función Pública para facilitar la implementación por parte de las entidades, publica y actualiza periódicamente el Manual Operativo MIPG, documento que brinda los elementos fundamentales para que las entidades públicas implementen el Modelo de manera adecuada y fácil, ya que contempla los aspectos generales que se deben tener en cuenta para cada una de las políticas de gestión y desempeño tal como su marco normativo, su ámbito de aplicación, sus propósitos, sus lineamientos generales y los criterios diferenciales para aplicar en las entidades territoriales.

Para garantizar que la Escuela contra la Drogadicción utilice la información detallada y actualizada del MIPG, esta debe ser consultada desde el micrositio web de MIPG, través del enlace https://www.funcionpublica.gov.co/web/MIPG

[1] FUNCION PUBLICA. Manual operativo MIPG, versión 5, marzo 2023. p. 9.

1. OBJETIVO

Este documento contiene los elementos fundamentales para que la Escuela Contra La Drogadicción implemente la Política de Seguridad Digital (información e informática) que se deben seguir por parte de los empleados públicos y contratistas de la Escuela con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

2. RESPONSABILIDADES EN LA IMPLEMENTACION DE LA POLITICA

El Comité Institucional de Gestión y Desempeño de la Escuela contra la Drogadicción ha designado como líderes de la implementación de la Política de Seguridad Digital los siguientes cargos:

- Profesional Ingeniero de Sistemas

Responsabilidad de los líderes de implementación de la política:

- Asegurarse que se incluya en los programas de inducción y reinducción el desarrollo del curso virtual sobre MIPG disponible en el Aula Virtual del Estado Colombiano[2], en el enlace/web/eva/curso-mipg, de la siguiente manera: El módulo "Fundamentos Generales" para todos los servidores públicos y para los responsables de la implementación de la política la totalidad de los módulos.

- Identificar oportunamente actualizaciones del MIPG relacionadas con la implementación de la política, revisando periódicamente el micrositio web de MIPG en el enlace https://www.funcionpublica.gov.co/web/MIPG y realizar los ajustes necesarios en los documentos pertinentes y socializar entre el personal al que aplique el cambio.

- Mantener relacionamiento con Función Púbica y el Conglomerado Público de la Gobernación, instituciones que apoyan y facilitan la implementación del MIPG y del Modelo de Gerencia Pública en Antioquia.

- Realizar autodiagnóstico del avance de la política en compañía de su equipo de trabajo, conforme a las herramientas vigentes dispuestas por Función Pública.

- Formular y garantizar la ejecución de las acciones para avanzar en la implementación de la política, adaptando a las circunstancias de la Escuela los lineamientos para la implementación definidos por la Función Pública en el Manual Operativo MIPG vigente.

[2] FUNCION PUBLICA. Circular No 100.04-2018

3. METODOLOGIA PARA LA IMPLEMENTACION DE LA POLITICA:

Siguiendo la metodología establecida en el Manual Operativo MIPG y utilizando guías y herramientas dispuestas por la Función Pública en el micrositio web https://www.funcionpublica.gov.co/web/MIPG, se deben realizar las siguientes etapas:

- **Autodiagnóstico:** se lleva a cabo utilizando la herramienta de autodiagnóstico en Excel, este ejercicio arroja la calificación gráfica y numérica entre 0 y 100 del cumplimiento de la política y sus respectivos componentes y categorías. Debe hacerse al menos una vez al año, es recomendable hacerlo entre octubre y noviembre.

- **Priorización de objetivos y metas**: con base en los resultados del autodiagnóstico se recomienda darle prioridad a aquellas actividades que obtuvieron menores puntajes y que se encuentran en color rojo, naranja y amarillo, que representan las debilidades. Es recomendable hacerlo a más tardar en noviembre.

- **Formulación de plan de acción:** para las debilidades priorizadas se formula un plan que contenga las estrategias, acciones y responsables, se aseguran los recursos necesarios y se definen tiempos de ejecución y cumplimiento para ejecutar lo planeado. Para la formulación de las acciones es muy importante considerar que la Escuela contra la Drogadicción se encuentra en un nivel básico de madurez según el Indice de Desempeño Institucional (46.3 según la evaluación FURAG 2021) y por tanto hay mucho hacer, sin embargo, también es necesario tener en cuenta que la Escuela tiene una planta de personal y un presupuesto ajustado, razón por la cual deben incluirse en la planeación anual acciones viables de lograr durante la vigencia siguiente. Estos planes de acción para el cumplimiento de políticas se pueden integrar con los planes institucionales y estratégicos de que trata el Decreto 612 de 2018. Es recomendable formular planes a más tardar en enero de la vigencia siguiente.

- **Ejecución y seguimiento del plan de acción:** la entidad ejecuta las actividades planeadas para lograr los resultados y metas a través de procesos y procedimientos claros y una estructura organizacional adecuada, optimizando el uso de recursos y de las TIC. El responsable de liderar la política debe realizar seguimiento trimestral a la ejecución y presentar ante el Comité de Gestión y Desempeño el avance.

4. RELACION DE LA POLITICA DE SEGURIDAD DIGITAL CON LA DIMENSION DEL MIPG

MIPG opera a través de la puesta en marcha de siete dimensiones que al ser puestas en marcha de manera articulada e intercomunicada permitirán a la Escuela Contra La Drogadicción la implementación del Modelo de forma adecuada y sencilla y generar valor público. La Política de Seguridad Digital se articula con otras para lograr el objetivo de la Dimensión Gestión con valores para resultados:

Que busca la Dimensión MIPG	Políticas mediante las cuales se desarrolla la dimensión
MIPG facilita que la gestión de las entidades esté orientada hacia el logro de resultados en el marco de la integridad. Para esto, pone en marcha los cursos de acción o trayectorias de implementación definidas en la dimensión de Direccionamiento Estratégico y Planeación y contando con el talento humano disponible en la entidad	Transparencia, acceso a la información pública y lucha contra la corrupción
	Fortalecimiento organizacional y simplificación de procesos
	Servicio al ciudadano
	Participación ciudadana en la gestión pública
	Racionalización de trámites (no aplicable a la Escuela contra la Drogadicción)
	Gobierno digital
	Seguridad digital
	Defensa jurídica
	Mejora normativa (no aplicable a la Escuela contra la Drogadicción)

5. PROPOSITO DE LA POLITICA DE SEGURIDAD DIGITAL[3]

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. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país.

6. MARCO NORMATIVO[4]

- ✓ Ley 1928 de 2018 "por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia"
- ✓ Conpes 3854 de 2016 "Política nacional de seguridad digital"
- ✓ Decreto 1078 de 2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
- ✓ Ley 1712 de 2014 "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"
- ✓ Ley estatutaria 1581 del 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"
- ✓ Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien 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"

[3] FUNCION PUBLICA. Manual Operativo MIPG, versión 5, marzo 2023. p. 74
[4] Idem, p. 74

7. LINEAMIENTOS PARA LA IMPLEMENTACION

A continuación, se presentan los principales elementos que facilitarán la implementación de la Política de Seguridad Digital. El detalle se encuentra en el Manual Operativo MIPG y las guías de apoyo dispuestas por la Función Pública.

Actualmente los lineamientos para la implementación se encuentran en reformulación por parte del MINTIC, en tanto se generan los nuevos lineamientos, la Escuela contra la Drogadicción tendrá como lineamientos de política los siguientes.

7.1 Política de organización interna

Establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la Escuela Contra La Drogadicción por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de TIC, buscando preservar la confidencialidad, integridad y disponibilidad de la información.

Alcance: La Política de Organización Interna aplica a todos los funcionarios y terceros (contratistas) de la Escuela Contra La Drogadicción.

7.2 Política para dispositivos móviles

Establecer los lineamientos para el buen uso y administración de los equipos de computación y comunicación móvil asignados o autorizados a los funcionarios de la Escuela Contra La Drogadicción, para el desarrollo de sus funciones, y así asegurar la confidencialidad, la integridad y la disponibilidad de la información de la Escuela contenida en estos.

Alcance: todos los colaboradores y terceros que utilicen dispositivos móviles para acceder a los servicios ofrecidos por la Escuela (red, Internet, correo electrónico, sistemas de información etc.)

7.3 Política de Teletrabajo

Proteger la información de la Escuela Contra La Drogadicción a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.

Alcance: La política de teletrabajo aplica para los empleados (funcionarios de planta) de la Escuela Contra La Drogadicción con quienes se establezca un contrato de trabajo que, para su ejecución, se realice mediante el teletrabajo.

7.4 Política de trabajo remoto.

Proteger la información de la ECD a la que se tiene acceso y aquella que es procesada o almacenada en los lugares en los que se realiza el trabajo remoto por parte de los funcionarios y terceros (contratistas de prestación de servicios) que lo requieran y estén autorizados.

Alcance: todos los funcionarios y terceros de la ECD que requieran por su tipo de contrato acceder a los servicios tecnológicos ofrecidos por el ECD (conectar sus equipos móviles, ingresar a la red, internet, correo electrónico, sistemas de información, acceder a la información etc.), en un sitio diferente a las instalaciones de la Escuela.

7.5 Política de seguridad de los recursos humanos

Asegurar que los funcionarios y terceros comprendan y alcancen conciencia sobre sus responsabilidades de seguridad de la información y las cumplan, además asegurar que son idóneos en los roles asignados y que se protegen los intereses de la ECD como parte del proceso de cambio de vinculación o terminación de esta.

Alcance: debe ser cumplida por todos los funcionarios y terceros de todos los procesos de la ECD; cubre los objetivos de control (Norma ISO 27001): antes de asumir, durante la ejecución y la terminación o cambio de la vinculación a la ECD.

7.6 Política de uso adecuado de los recursos

Dar un buen uso a los recursos: correo electrónico, internet, redes sociales, recursos tecnológicos (Equipo de cómputo), uso de software legal y derechos de autor, acceso inalámbrico que provee la ECD a todos los funcionarios y terceros para el cumplimiento de sus funciones u obligaciones, y para proteger la información de la ECD.

Alcance: Aplica para todos los funcionarios y terceros vinculados con la ECD que tienen acceso a los servicios de correo electrónico, acceso a internet, redes sociales, recursos tecnológicos (Equipos de cómputo), uso de software legal y derechos de autor, acceso inalámbrico para el desarrollo de sus funciones.

7.7 Política de gestión de activos de información

Identificar los activos de información de la ECD para definir las responsabilidades de protección apropiadas y clasificarlas para asegurar que la información de la ECD recibe un nivel apropiado de protección, de acuerdo con su importancia, y se efectúe un manejo adecuado de los medios para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de la información de la Escuela almacenada en ellos.

Alcance: Aplica para los activos de información de todos los procesos de la ECD.

7.8 Política de control de acceso.

Definir las directrices generales para un acceso controlado a servicios de tecnología (Red, servicios asociados, sistemas de información) e información de la ECD.

Alcance: aplica para todos los funcionarios y terceros que cuenten con accesos a los servicios de tecnología (Red, servicios asociados, sistemas de información) e información de la ECD.

7.9 Política sobre controles criptográficos

Buscar que se dé un uso adecuado y eficaz de sistemas y técnicas criptográficas para la protección de la información de la ECD, con base al análisis de riesgo efectuado, con el fin de asegurar la protección de su confidencialidad e integridad.

Alcance: aplica para las comunicaciones, bases de datos y unidades de disco duros de los equipos de cómputo portátiles con que cuenta la ECD.

7.10 Política de seguridad física y del entorno

Minimizar los riesgos de daños e interferencias a la información y a las operaciones de la ECD, evitando accesos físicos no autorizados a las instalaciones de procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información de la ECD.

Alcance: aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de archivo, áreas de recepción, tesorería, dirección y entrega de correspondencia, las cuales deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la información de la ECD.

7.11 Política de escritorio y pantalla limpias

Mantener el escritorio y la pantalla despejada, con el fin de reducir el riesgo de acceso no autorizado, pérdida y daño de la información de la ECD.

Alcance: aplica para todos los funcionarios y terceros de la ECD.

7.12 Política de seguridad de las operaciones

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información de la ECD.

Alcance: aplica para la OTSI de la ECD.

7.13 Política de gestión de seguridad de las redes.

Fortalecer la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte de la ECD.

Alcance: Esta política aplica para todas las redes, los servicios de red y los controles utilizados para proteger la información en la transferencia de información de la ECD.

7.14 Política de intercambio de información.

Proteger la transferencia de información de la ECD mediante el uso de todo tipo de instalaciones de comunicación, como correo electrónico, VPN, SFTP (protocolo de transferencia segura de archivos), etc.

Alcance: aplica para la información que sea enviada por los funcionarios a través de correo electrónico y los demás canales que se autoricen VPN, SFTP, etc.

3.15 Política de adquisición, desarrollo y mantenimiento de sistemas

Fortalecer la seguridad digital y que sea una parte integral de los sistemas de información de la ECD durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.

Alcance: aplica para todos los sistemas de información de la ECD, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

7.16 Política de seguridad de la información para las relaciones con proveedores

Buscar la protección de los activos información de la ECD que sean accesibles a los proveedores.

Alcance: aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica de la ECD.

7.17 Política de gestión de incidentes y mejoras en la seguridad digital

Gestionar todos los incidentes de seguridad digital reportados en la ECD, adecuadamente, dando cumplimiento a los procedimientos establecidos.

Alcance: aplica para todos los funcionarios y terceros de la ECD que detecten un evento o incidente de seguridad digital el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos en la ECD.

GERARDO VANEGAS JARAMILLO
Subdirector Administrativo Financiero ECD
Secretario Comité de Gestión y Desempeño

FABIO VILLA RODRIGUEZ
Director Escuela Contra La Drogadicción
Presidente Comité de Gestión y Desempeño