Políticas de Seguridad Digital

Tabla de contenido

1 Objetivo

Definir las políticas de seguridad digital (información e informática) que se deben seguir por parte de los colaboradores y terceros del MEN, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información.

2 Alcance

Las políticas y directrices definidas en el presente Manual aplican para todos los colaboradores y terceros del MEN. Las directrices, responsables y soportes detallados se encuentran en la guía respectiva de cada política (Consultar en la aplicación del SIG).

3 Definiciones

- **MSPI:** Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información y las Telecomunicaciones – MINTIC.
- **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.
- **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.
- **Confidencialidad:** Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas 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.
- **Dato:** Es una representación simbólica (numérica, alfabética, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **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.
- **Servidor:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta apropiada.
- **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.

- **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.
- **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.
- **File Server:** Es un servidor de archivos que almacena y distribuye diferentes tipos de archivos informáticos del MEN.
- **Información confidencial o crítica:** Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en el MEN
- **MEN:** Ministerio de Educación Nacional
- **Mesa de Ayuda de Tecnología:** Centro de Atención al Usuario mediante el cual la OTSI presta servicios para gestionar y atender de requerimientos relacionados con los servicios TIC en el MEN.
- **OneDrive:** Plataforma en la nube de Microsoft que permite guardar los archivos o documentos (Ejemplo: información pública de las áreas del MEN) en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet.
- **OTSI:** Oficina de Tecnología y Sistemas de Información del MEN
- **Cuota (*quota*):** Límite, establecido por el administrador a cada usuario, para la asignación de espacio en el disco duro para almacenamiento de la información de la institución.
- **SharePoint:** Sitio web que ofrece un espacio central de colaboración y almacenamiento de documentos, información e ideas.
- **SGSI:** Sistema de Gestión de Seguridad de la Información del MEN.
- **Seguridad digital:** Es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante,

incluye la seguridad de la información (Políticas, Procedimientos y demás controles) y la seguridad informática (Herramientas de seguridad).

- **Teletrabajo:** Todas las formas de trabajo por fuera de la oficina, incluidos los entornos de trabajo no tradicionales, a los que se denomina "trabajo a distancia", "lugar de trabajo flexible", "trabajo remoto" y ambientes de "trabajo virtual".
- **Dispositivos móviles:** son aquellos dispositivos (portátiles, tablets y teléfonos móviles) que nos facilitan trabajar fuera de las instalaciones del MEN.

4 Políticas de Seguridad Digital

4.1 Política de organización interna

Establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior del MEN 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 colaboradores y terceros del MEN

4.2 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 colaboradores del MEN, para el desarrollo de sus funciones, y así asegurar la confidencialidad, la integridad y la disponibilidad de la información del MEN contenida en estos.

Alcance

La política para uso de dispositivos móviles será aplicada por la OTSI, a todos los colaboradores y terceros que utilicen dispositivos móviles para acceder a los servicios ofrecidos por el MEN (red, Internet, correo electrónico, sistemas de información etc.)

4.3 Política de Teletrabajo

Proteger la información del MEN 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 colaboradores (funcionarios de planta) del MEN con quienes se establezca un contrato de trabajo que, para su ejecución, se realice mediante el teletrabajo.

4.4 Política de trabajo remoto

Proteger la información del MEN 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 colaboradores y terceros que lo requieran y estén autorizados.

Alcance

La política de trabajo remoto será aplicada por la OTSI, a todos los colaboradores y terceros del MEN que requieran por su tipo de contrato acceder a los servicios tecnológicos ofrecidos por el MEN (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 del Ministerio.

4.5 Política de seguridad de los recursos humanos

Asegurar que los colaboradores y terceros comprendan y toman 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 del MEN como parte del proceso de cambio de vinculación o terminación de esta.

Alcance

La política de seguridad de los recursos humanos debe ser cumplida por todos los colaboradores y terceros de todos los procesos del MEN; cubre los objetivos de control (Norma ISO 27001): antes de asumir, durante la ejecución y la terminación o cambio de la vinculación al MEN.

4.6 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 el MEN a todos los colaboradores y terceros para el cumplimiento de sus funciones u obligaciones, y para proteger la información del MEN.

Alcance

Aplica para todos los colaboradores y terceros vinculados con el MEN 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.

4.7 Política de gestión de activos de información

Identificar los activos de información del MEN para definir las responsabilidades de protección apropiadas y clasificarlas para asegurar que la información del MEN 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 del Ministerio almacenada en ellos.

Alcance

Aplica para los activos de información de todos los procesos del MEN

4.8 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 del MEN.

Alcance

Esta política aplica para todos los colaboradores y terceros que cuenten con accesos a los servicios de tecnología (Red, servicios asociados, sistemas de información) e información del MEN.

4.9 Política sobre controles criptográficos

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

Alcance

La política de controles criptográficos aplica para las comunicaciones, bases de datos y unidades de disco duros de los equipos de cómputo portátiles con que cuenta el MEN.

4.10 Política de seguridad física y del entorno

Minimizar los riesgos de daños e interferencias a la información y a las operaciones del MEN, evitando accesos físicos no autorizados a las instalaciones de

procesamiento de información, que atenten contra la confidencialidad, integridad o disponibilidad de la información del MEN.

Alcance

Esta política 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, despachos 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 del MEN.

4.11 Política de escritorio y pantalla limpios

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

Alcance

Esta política aplica para todos los colaboradores y terceros del MEN.

4.12 Política de seguridad de las operaciones

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información del MEN.

Alcance

Esta política aplica para la OTSI del MEN,

4.13 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 del MEN

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 del MEN.

4.14 Política de intercambio de información

Proteger la transferencia de información del MEN mediante el uso de todo tipo de instalaciones de comunicación, como correo electrónico, VPN, SFTP, etc.

Alcance

Esta política de intercambio de información aplica para la información que sea enviada por los colaboradores a través de correo electrónico y los demás canales que se autoricen VPN, SFTP, etc.

4.15 Política de adquisición, desarrollo y mantenimiento de sistemas

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

Alcance

Esta política aplica para todos los sistemas de información del MEN, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

4.16 Política de desarrollo seguro

Propender porque la seguridad digital esté diseñada e implementada dentro del ciclo de vida planeación y desarrollo de los sistemas de información.

Alcance

Esta política aplica para todos los desarrollos de sistemas de información en el MEN.

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

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

Alcance

Esta política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica del MEN.

4.18 Política de gestión de incidentes y mejoras en la seguridad digital.

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

Alcance

Esta política aplica para todos los colaboradores y terceros del MEN que detecten un evento o incidente de seguridad digital el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos en el MEN.

5 Información de contacto

Cualquier inquietud relacionada con las políticas, favor remitirla al correo seguridaddigital@mineducacion.edu.co.

6 Revisión de las políticas de Seguridad Digital

Estas políticas deben ser revisadas por la OTSI como mínimo una vez al año.

7 Referentes normativos

7.1.1 Referentes de políticas del MEN

- Manual del Sistema Integrado de Gestión – MEN,Sistema de Gestión de Seguridad de la Información

7.1.2 Referentes de política nacional

- Manual de seguridad y privacidad de la información – Min TIC - Estrategia de Gobierno Digital.
- Norma técnica Colombiana NTC-iso/iec 27001

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
Política de organización interna	Dominio A.6.1 Organización interna Controles: A.6.1.1, A.6.1.2, A.6.1.3, A.6.1.4, A.6.1.5	Guía no 2 - Política General MSPI Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información. Inventario
Política para dispositivos móviles	Dominio A.6.2 Dispositivos móviles y teletrabajo: Controles A.6.2.1	Guía no 2 - Política General MSPI
Política de teletrabajo	Dominio A.6.2 Dispositivos móviles y teletrabajo – Controles A.6.2.2	Guía no 2 - Política General MSPI
Política de trabajo remoto	Dominio A.6.2 Dispositivos móviles y teletrabajo – Controles A.6.2.2	Guía no 2 - Política General MSPI
Política de seguridad de los recursos humanos	Dominio A.7 Seguridad de los recursos humanos	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
	Controles A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1	
Política de uso adecuado de los recursos	Dominio A.7 Seguridad de los recursos humanos Controles: A.7.2.2	Guía no 2 - Política General MSPI
Política de seguridad de los recursos humanos	Dominio A.7 Seguridad de los recursos humanos Controles A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2., A.7.3.	Guía no 2 - Política General MSPI
Política de uso adecuado de los recursos	Dominio A.7 Seguridad de los recursos humanos Objetivo de control A.7.2 Durante la ejecución del empleo Controles A.7.2.2	Guía no 2 - Política General MSPI
Política de gestión de activos	Dominio A.8 Gestión de activos. Controles A.8.1.1, A.8.1.2, A.8.1.3, A.8.1.3, A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3	Guía no 2 - Política General MSPI
Política de control de acceso	Dominio A.9 Control de acceso Controles A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.3	Guía no 2 - Política General MSPI
Política de controles criptográficos	Dominio A.10 Criptografía Controles A.10.1.1, A.10.1.2	Guía no 2 - Política General MSPI
Política de seguridad física y del entorno	Dominio A.11 Seguridad física y del entorno Controles	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
	A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5 A.11.2.1, A.11.2.2, A.11.2.3 A.11.2.4, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8., A.11.1.3 A.11.1.6	
Política de escritorio limpio y pantalla limpia	Dominio A.11 Seguridad física y del entorno Control A.11.2.9	Guía no 2 - Política General MSPI
Política de seguridad de las operaciones	Dominio A.12 Seguridad de las operaciones Controles A.12.1.1, A.12.1.2, A.12.1.3, A.12.1.4, A.12.2.1, A.12.3.1, A.12.4.1, A.12.4.3, A.12.4.4, A.12.5.1, A.12.6.1, A.12.6.2, A.12.7	Guía no 2 - Política General MSPI
Política de seguridad de las comunicaciones	Dominio A.13 Seguridad de las comunicaciones Controles A.13.1.1, A.13.1.2, A.13.1.3 .13.2.1, A.13.2.2 A.13.2.3, A.13.2.4	Guía no 2 - Política General MSPI
Política de adquisición, desarrollo y mantenimiento de sistemas	Dominio A.14 Adquisición, desarrollo y mantenimiento de sistemas Objetivo de control A.14.1 Requisitos de seguridad en los sistemas de información Controles	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
	A.14.1.1, A.14.1.2, A.14.1.3	
Política de desarrollo seguro	Dominio A.14, A.14.2 A.14.2.1, A.14.2.2, A.14.2.3, A.14.2.4, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1	Guía no 2 - Política General MSPI
Política de seguridad de la información para las relaciones con proveedores	Dominio A.15 Objetivo de control A.15.1 Controles A.15.1.1, A.15.1.2 A.15.1.3, A.15.2 A.15.2.1 A.15.2.2	Guía no 2 - Política General MSPI
Política de gestión de incidentes y mejoras en la seguridad digital.	Dominio A.16 Gestión de incidentes de seguridad de la información Objetivo de control A.16.1 Controles A.16.1.1, A.16.1.2, A.16.1.3, A.16.1.4, A.16.1.5, A.16.1.6, A.16.1.7.	Guía no 2 - Política General MSPI
Política de seguridad de la información en la continuidad de negocio.	Dominio A.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio Objetivo de control A.17.1 Continuidad de seguridad de la información Controles	Guía no 2 - Política General MSPI

Política definida en el manual	Control ISO27001	Modelo de Seguridad y Privacidad Min TIC
	A.17.1.1, A.17.1.2, A.17.1.3 A.17.2, A.17.2.1	
Política cumplimiento de requisitos legales y contractuales	Dominio A.18 Cumplimiento Objetivo de control A.18.1 Cumplimiento de requisitos legales y contractuales Controles A.18.1.1, A.18.1.2 A.18.1.3, A.18.1.4 A.18.1.5. A.18.2.1, A.18.2.2 A.18.2.3	Guía no 2 - Política General MSPI

Control de Cambios		
Versión	**Fecha de vigencia**	**Naturaleza del cambio**
01	A partir de su publicación en el SIG	Se unificó el manual de seguridad informática y el manual de políticas de seguridad de la información y se creó una guía por cada política para especificar las directrices, responsables y soportes.

Registro de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Luis Carlos Serrano Pinzon	**Nombre**	Lina Mercedes Durán Martínez	**Nombre**	Roger Quirama Garcia
Cargo	Contratista de la Oficina de Tecnologia y Sistemas de Información	**Cargo**	Profesional Especializado - Subdirección de Desarrollo Organizacional.	**Cargo**	Jefe de la Oficina de Tecnologia y Sistemas de Información