



La educación
es de todos

Mineducación

**GUÍA - POLÍTICA DE GESTIÓN DE
SEGURIDAD DE LAS REDES**

Código: ST-GU-12

Versión: 1

Rige a partir de su publicación
en el SIG

Política de gestión de seguridad de las redes

Tabla de contenido

1	Objetivo.....	3
2	Alcance	3
3	Definiciones.....	3
4.	Directrices	4
4.1	Gestión de la seguridad de las redes.....	4
4.1.1	Controles de redes	4
4.1.2	Seguridad de los servicios de red.....	5
4.1.3	Separación en las redes	6
5.	Información de contacto.....	7
6.	Revisión de la guía	7
7.	Referentes.....	7
7.1	Referentes Normativos.....	7
7.1.1	Referentes de política nacional	7
7.1.2	Referentes de políticas del Ministerio de Educación Nacional	7

1 Objetivo

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

2 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.

3 Definiciones

- **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.
- **Activo de Información:** Es todo aquello que en el Ministerio de Educación Nacional es considerado importante o de alto valor para la entidad, 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.
- **SGSI:** Sistema de Gestión de Seguridad de la Información.
- **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)

4. Directrices

4.1 Gestión de la seguridad de las redes

4.1.1 Controles de redes

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Gestionar y controlar las redes para proteger la información en sistemas y aplicaciones.	Administrar y gestionar la red del MEN.	Oficina de Tecnología y Sistemas de Información	log Cisco Identity Services Engine (ISE)
	Establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.		log Cisco Identity Services Engine (ISE)
	Proporcionar a los colaboradores y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales.		Soportes contractuales
	Monitorear la funcionalidad de las redes a través del uso de analizadores de red.		Soportes monitoreo Cisco Identity Services Engine (ISE)
	No es permitido conectar a las estaciones de trabajo o a los puntos de acceso de la red corporativa, elementos de red (tales como switches, enrutadores, módems, etc.) que no sean autorizados por la OTSI.	Todos los colaboradores y terceros del MEN	NA

4.1.2 Seguridad de los servicios de red

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
<p>Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.</p>	<p>Dar el acceso a internet exclusivamente a través de la red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.</p>	<p>Oficina de Tecnología y Sistemas de Información</p>	<p>Log del Firewall</p>
	<p>Administrar la habilitación y/o bajas de los dispositivos móviles (computadoras portátiles, Ipad, celulares, etc.) propiedad del MEN y de los usuarios que hayan sido solicitados a través de la mesa de ayuda de tecnología.</p>		<p>Log Cisco Identity Services Engine (ISE)</p>
	<p>Utilizar el acceso a la red, Internet, exclusivamente para el desarrollo de sus actividades propias de las funciones desempeñadas en el MEN.</p>	<p>Todos los colaboradores del MEN</p>	<p>N.a.</p>
	<p>Usar la red inalámbrica del MEN, para lo cual necesariamente deberá estar dentro del dominio del MEN y tener instalado el programa informático ISE.</p>		<p>N.a.</p>
	<p>El acceso de los colaboradores a la red debe realizarse a través de la red inalámbrica definida como (MINISTERIO) o mediante la red cableada</p>		<p>N.a</p>
	<p>Conectarse única y exclusivamente a la red inalámbrica (Invitados) del MEN a internet sin la necesidad de algún tipo de cableado. La red inalámbrica de invitados le permitirá utilizar los servicios de internet, en las zonas de cobertura del MEN.</p>	<p>Clientes, Proveedores, Visitantes del MEN</p>	<p>N.a</p>
	<p>Los usuarios que accedan a través de la red invitados no tendrán acceso a los servicios, sistemas de información, etc., del MEN ni a ningún recurso de uso privado del MEN</p>		<p>Log Cisco Identity Services Engine (ISE)</p>

4.1.3 Separación en las redes

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Separar en las redes los grupos de servicios de información, usuarios y sistemas de información	Establecer un esquema de segregación de redes, con el fin de controlar el acceso a los diferentes segmentos de red y buscar que se preserve la confidencialidad, integridad y disponibilidad de la información del MEN.	Oficina de Tecnología y Sistemas de Información	Logs switches
	Establecer parámetros técnicos para la conexión segura de la red con los servicios de red.		Logs switches
	Establecer mecanismos de autenticación seguros para el acceso a la red.		Log Cisco Identity Services Engine (ISE)
	Separar las redes inalámbricas públicas de las redes internas, para preservar los principios de la seguridad de la información.		Log Cisco Identity Services Engine (ISE)

5. Información de contacto

Cualquier inquietud relacionada con la guía política de gestión de seguridad de las redes, favor remitirla al correo seguridaddigital@mineducacion.edu.co

6. Revisión de la guía

Esta política debe ser revisada periódicamente por la OTSI como mínimo una vez al año.

7. Referentes

7.1 Referentes Normativos

Norma ISO 27001

Dominio A.13. Gestión de la seguridad de las redes

7.1.1 Referentes de política nacional

Manual de seguridad y privacidad de la información – Min TIC - Estrategia de Gobierno Digital.
Numeral 8.2 Fase de planificación - Políticas de Seguridad y Privacidad de la Información

-

7.1.2 Referentes de políticas del Ministerio de Educación Nacional

- Otras políticas asociadas que tenga definida la entidad dentro del MSPI
- Manual del Sistema Integrado de Gestión – MEN. Sistema de Gestión de Seguridad de la Información

Control de Cambios		
Versión	Fecha de vigencia	Naturaleza del cambio
01	A partir de su publicación	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 Pinzón	Nombre	Lina Mercedes Durán Martínez	Nombre	Roger Quirama Garcia
Cargo	Contratista de la Oficina de Tecnología y Sistemas de Información	Cargo	Profesional Especializado - Subdirección de Desarrollo Organizacional.	Cargo	Jefe de la Oficina de Tecnología y Sistemas de Información