



# **Guía - Política sobre el uso de controles criptográficos**



## Tabla de contenido

1	Objetivo.....	3
2	Alcance.....	3
3	Definiciones.....	3
4.	Directrices.....	4
4.1	Controles criptográficos.....	4
4.1.1	Uso de controles criptográficos.....	4
4.1.2	Gestión de llaves.....	5
5.	Información de contacto.....	6
6.	Revisión de la guía.....	6
7.	Referentes.....	6
7.1	Referentes Normativos.....	6
7.1.1	Referentes de política nacional.....	6
7.1.2	Referentes de políticas del MEN.....	6

## 1 Objetivo

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información del MEN.

## 2 Alcance

Lo definido en la presente guía política sobre controles criptográficos aplica para las comunicaciones, bases de datos y unidades de disco duro de los equipos de cómputo portátiles con que cuenta el 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.
- **Criptografía:** Se ocupa del estudio de los algoritmos, protocolos y sistemas que se utilizan para proteger la información y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- **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.
- **MEN:** Ministerio de Educación Nacional
- **OTSI:** Oficina de Tecnología y Sistemas de Información del MEN
- **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).
- **SGSI:** Sistema de Gestión de Seguridad de la Información.

#### 4. Directrices

##### 4.1 Controles criptográficos

##### 4.1.1 Uso de controles criptográficos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información	Aplicar la política de controles criptográficos por medio de su operador de servicios TIC y la herramienta de encriptación definida en: <ul style="list-style-type: none"> <li>• Las unidades de disco duros de los equipos de cómputo portátiles con que cuenta el MEN.</li> <li>• Claves de acceso a sistemas, datos y servicios.</li> <li>• Información digital reservada y clasificada.</li> <li>• Correos electrónicos con información reservada y clasificada.</li> </ul>	OTSI	Soportes de implementación de los controles de encriptación
	Verificar que todo sistema de información que requiera realizar transmisión de información clasificada o reservada cuente con mecanismos de cifrado de datos.		Soportes de Verificación
	Utilizar controles criptográficos para la transmisión de información clasificada o reservada, fuera del ámbito del Ministerio.		Soportes de encriptación en las trasmisiones de información.
	Asegurar que los sistemas de información tengan establecidos los controles criptográficos cumpliendo los estándares establecidos por el Ministerio.		Soportes de Verificación
	Disponer de herramientas que permitan el cifrado de la información sobre los medios de almacenamiento de esta.		Medios de almacenamiento de información.

#### 4.1.2 Gestión de llaves

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
<p>Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.</p>	<p>Comunicar por medio de la mesa de ayuda de tecnología para solicitar el cambio de contraseña de la sesión de usuario en caso de que la olvide. (Dado que para el caso de los equipos de cómputo portátiles la</p>	<p>Todos los colaboradores del MEN</p>	<p>Mesa de ayuda de tecnología</p>
	<p>Comunicar por medio de la mesa de ayuda de tecnología, la solicitud para obtener de nuevo su información, en caso de que al ingresar al sistema realice más de tres intentos de inicio de sesión, dado que en estos casos el disco duro del equipo de cómputo portátil será cifrado.</p>		<p>Mesa de ayuda de tecnología</p>
	<p>En el caso de las contraseñas de encriptación de información asociadas a los equipos de cómputo portátiles, el MEN utiliza las mismas contraseñas de las sesiones de usuario.</p>	<p>OTSI</p>	<p>Servidor de dominio del MEN.</p>
	<p>Desbloquear contraseña de los usuarios atendiendo requerimiento del olvido de contraseña a través de la mesa de ayuda de tecnología.</p>		<p>Mesa de ayuda de tecnología</p>
	<p>Restablecer la información de los usuarios atendiendo requerimiento a través de la mesa de ayuda de tecnología en caso de que el disco duro sea cifrado por intento de acceso fallido.</p>		<p>Mesa de ayuda de tecnología</p>
	<p>La asignación del tiempo de vida de las llaves criptográficas la realiza el usuario administrador de dominio del directorio activo, de acuerdo con el contexto y particularidades en el momento de la asignación. <b>(Revisar para desagregar de acuerdo con oportunidad de mejora)</b></p>		<p>Contratos de adquisición de llaves criptográficas.</p>

## 5. Información de contacto

Cualquier inquietud relacionada con la Guía política sobre el uso de controles criptográficos, favor remitirla al correo [seguriddigital@mineducacion.edu.co](mailto:seguriddigital@mineducacion.edu.co).

## 6. Revisión de la guía

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

## 7. Referentes

### 7.1 Referentes Normativos

- Norma ISO 27001
- Dominio A.10 Criptografía

#### 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 MEN

- 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 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	
<b>Nombre</b>	Luis Carlos Serrano Pinzón	<b>Nombre</b>	Lidy Milene Pedraza Parra	<b>Nombre</b>	Roger Quirama Garcia
<b>Cargo</b>	Contratista de la Oficina de Tecnología y Sistemas de Información	<b>Cargo</b>	Profesional Especializado - Subdirección de Desarrollo Organizacional.	<b>Cargo</b>	Jefe de la Oficina de Tecnología y Sistemas de Información