Política de cumplimiento de requisitos legales y contractuales

Tabla de contenido

1 Objetivo

Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad en el MEN, y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al año o cuando se presente una actualización en la normatividad que afecte la seguridad de la información.

2 Alcance

La guía política de cumplimiento de requisitos legales y contractuales será aplicada por todas las dependencias del MEN, especialmente por la Secretaria General y la OTSI, además por todos los colaboradores y contratistas 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 alta validez 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.

- **Propiedad Intelectual:** es la denominación que recibe la protección legal sobre toda creación del talento o del ingenio humano, dentro del ámbito científico, literario, artístico, industrial o comercial. En el caso del Software, la legislación colombiana lo asimila a la escritura de una obra literaria, permitiendo que el código fuente de un programa esté cubierto por la ley de Derechos de Autor.

- **Derecho de Autor:** Se realiza sobre todas las formas en que se puede expresar las ideas, no requiere ningún registro y perdura durante toda la vida del autor, más 80 años después de su muerte, después de lo cual pasa a ser de dominio público. El registro de la obra ante la Dirección Nacional del Derecho de Autor sólo tiene como finalidad brindar mayor seguridad a los titulares del derecho.

- **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 Cumplimiento de los requisitos legales y contractuales

4.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Identificar y documentar explícitamente todos los requisitos estatutarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos y mantenerlos actualizados para cada sistema de información y para la organización	Documentar los controles y las responsabilidades individuales para cumplir estos requisitos estatutarios, reglamentarios y contractuales	Oficina de Tecnología y Sistemas de Información	Formato roles y responsabilidades
	Identificar toda la legislación aplicable al MEN para cumplir los requisitos del Ministerio de educación Nacional	Líderes de proceso del MEN	Normograma
	Identificar y documentar explícitamente todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque del MEN para cumplirlos y mantenerlos actualizados para cada sistema de información y para el MEN.		Normograma

4.1.2 Derechos de propiedad intelectual

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados	Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	Oficina de Tecnología y Sistemas de Información	Documentación asociada al proceso Gestión de Servicios TIC
	✓ Asegurar la protección de cualquier material que se pueda considerar propiedad intelectual, teniendo en cuenta los siguientes lineamientos: o Publicar una política de cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos. o Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor. o Mantener conciencia de las políticas para proteger los derechos de propiedad intelectual y notificar la intención de tomar acciones disciplinarias contra el personal que las incumpla. o Mantener los registros de activos apropiados, e identificar todos los activos con requisitos para proteger los derechos de propiedad intelectual. o Mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc. o Implementar controles para asegurar que no se exceda el número máximo de usuarios permitido dentro de cada licencia. o Llevar a cabo revisiones para verificar que solo hay instalados software autorizado y productos con licencia. o Definir una política para mantener las condiciones de licencia apropiadas. o Definir una política para disposición o transferencia de software a terceros.		Guía derechos de autor

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Cumplir con los términos y condiciones para el software y la información obtenida de las redes públicas. ○ Duplicar, convertir a otro formato o extraer de registros comerciales solo lo que permita la ley de derechos de autor. ○ No copiar total ni parcialmente libros, artículos, reportajes u otros documentos diferentes de los permitidos por la ley de derechos de autor.		

4.1.3 Protección de registros

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Proteger los registros contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Proteger los registros (por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales) contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y del MEN.	Oficina de Tecnología y Sistemas de Información	Soportes controles y políticas SGSI
	Clasificar los registros por tipos, por ejemplo, registros contables, registros de bases de datos, logs de transacciones, logs de auditoría y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos, almacenamiento en nube. Cualquier llave criptográfica y programas relacionados asociados con archivos permanentes encriptados o firmas digitales, también se deben almacenar de manera segura para posibilitar la desencriptación de los registros durante el tiempo en que están retenidos.		Tablas de retención documental Clasificación de activos de información
	Para salvaguarda los registros, se deberían realizar los siguientes pasos dentro del MEN:	Gestión documental	Manual del sistema Integrado de

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Emitir directrices acerca de la retención, almacenamiento, manejo y disposición de registros e información. ○ Elaborar un programa de retención que identifique los registros y el período de tiempo durante el cual se deberían retener, de acuerdo con lo definido en las tablas de retención definidas por Gestión documental ○ Llevar un inventario de fuentes de información clave.		Conservación Procedimiento de actualización de las Tablas de Retención Documental TRD

4.1.4 Privacidad y protección de información de datos personales.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.	Desarrollar e implementar una política relativa a datos del MEN, para la privacidad y la protección de datos personales. Esta política se debe comunicar a todas las personas involucradas en el procesamiento de información de datos personales.	Oficina de Tecnología y Sistemas de Información	Manual - Política de Tratamiento de Datos Personales del MEN

4.1.5 Reglamentación de controles criptográficos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación reglamentación pertinentes.	Considerar los siguientes aspectos en relación con la conformidad con los acuerdos, leyes y reglamentaciones del MEN: ○ las restricciones sobre importación o exportación de hardware y software informático, para la realización de funciones criptográficas; ○ las restricciones sobre importación o exportación de hardware y software informático que está diseñado para la adición de funciones criptográficas; ○ las restricciones sobre el uso de la encriptación; ○ los métodos obligatorios o discrecionales de acceso por parte de las autoridades de los países a información encriptada mediante software o hardware para brindar confidencialidad al contenido.	Oficina de Tecnología y Sistemas de Información	Guía Política sobre el uso de controles criptográficos

4.2 Revisiones de seguridad de la información

4.2.1 Revisión independiente de la seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Revisar independientemente a intervalos planificados o cuando ocurran cambios significativos, el enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información).	Revisar de forma independiente a intervalos planificados, mínimo una vez al año o cuando ocurran cambios significativos la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información).	Oficina de Control Interno	Procedimiento Auditorías Internas - Control interno

4.2.2 Cumplimiento con las políticas y normas de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	Revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad digital apropiadas, y cualquier otro requisito de seguridad.	Los líderes de los procesos	Soportes Revisión por la Dirección

4.2.3 Revisión del cumplimiento técnico

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Revisar periódicamente los sistemas de información para determinar el cumplimiento con las políticas y normas de seguridad de la información.	✓ Revisar periódicamente, mínimo una vez al año, los sistemas de información para determinar el cumplimiento de las políticas y normas de seguridad de la información. ✓ Revisar preferiblemente con la ayuda de herramientas automáticas que generan informes técnicos para la interpretación posterior por un especialista técnico. Como alternativa, un ingeniero de sistemas experimentado puede llevar a cabo revisiones manuales (si es necesario, con el apoyo de herramientas de software apropiadas). o Si se usan pruebas de penetración o valoraciones de vulnerabilidad, es necesario tener precaución, ya que estas	Oficina de tecnología y sistemas de información	Informes de vulnerabilidades y pruebas de penetración

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	actividades pueden comprometer la seguridad del sistema. Estas pruebas se deben planificar, documentar, y deben ser repetibles. o Cualquier revisión de cumplimiento técnico solo podrá ser llevada a cabo por personas competentes autorizadas, o ser realizada bajo la supervisión de dichas personas.		

5. Información de contacto

Cualquier inquietud relacionada con la guía política de cumplimiento de requisitos legales y contractuales, favor remitirla al correo seguridaddigital@mineducacion.edu.co

6. Revisión de la guía

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

7. Referentes

7.1 Referentes Normativos

- Norma ISO 27001
- Dominio A.18. Cumplimiento

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