Política de gestión de incidentes de seguridad de la información

Tabla de contenido

1 Objetivo

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

2 Alcance

Esta política aplica para todos los colaboradores y terceros del MEN que detecten un evento o incidente de seguridad de la información el cual deben reportar, adecuadamente, de acuerdo con los procedimientos establecidos en 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.
- **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.
- **Evento de seguridad de la información:** Ocurrencia identificada de una condición de un proceso, sistema, servicio, red o del entorno que indica una posible violación de las políticas de seguridad de la información del Ministerio de Educación Nacional, o una falla en los controles o situación previamente desconocida que puede ser relevante para la seguridad de la información.
- **Incidente de seguridad de la información:** Uno o más eventos de seguridad de la información no deseados o inesperados que tienen una significativa

probabilidad de comprometer las operaciones de la entidad y amenazan la confidencialidad, integridad y/o disponibilidad de la información del Ministerio de Educación Nacional.

- **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, todo lo relacionado con esta y, especialmente, en 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 incidentes y mejoras de la seguridad de la información

4.1.1 Responsabilidades y procedimientos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	Establecer las responsabilidades en la gestión de incidentes de seguridad digital dentro del MEN.	Oficina de Tecnología y Sistemas de Información	Formato roles y responsabilidades SGI - Procedimiento gestión de incidentes
	Definir el procedimiento de atención de incidentes de seguridad de la información del MEN.		Procedimiento Gestión de Incidentes
	Dar un tratamiento adecuado a todos los incidentes de seguridad de la información reportados en el MEN.		Registro del reporte del incidente - Aplicación Modulo de Incidentes de seguridad de la información
	Realizar sensibilización a todos los colaboradores y terceros sobre incidentes de seguridad de la información.		Soportes actividades de sensibilización

4.1.2 Reporte de eventos de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Informar sobre los eventos de seguridad de la información a través de los canales de gestión apropiados, tan pronto como sea posible	Reportar de forma inmediata de acuerdo con el procedimiento previsto los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.	Todos los colaboradores y terceros del MEN	Registro del reporte del incidente - Aplicación Modulo de Incidentes de seguridad de la información

4.1.3 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evaluar los eventos de seguridad de la información y decidir si se van a clasificar	Evaluar cada evento o incidente de seguridad de la información presentado en el MEN, usando la escala de clasificación de eventos e incidentes de seguridad de la información con el fin de poder determinar clasificación y priorización. De acuerdo con el definido en el procedimiento previsto.	Oficina de Tecnología y Sistemas de Información	Registro de categorización del incidente de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Registrar los resultados de la evaluación y la decisión para referencia y verificación futuras (Lecciones aprendidas).		Informe de Gestión de Incidentes de Seguridad de la Información

4.1.4 Respuesta a incidentes de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados	Responder a los incidentes de seguridad de la información que se presenten en el MEN. La respuesta debe incluir lo siguiente: ✓ Recolectar evidencia lo más pronto posible después de que ocurra el incidente. ✓ Llevar a cabo análisis forense de seguridad de la información, según se requiera. ✓ Llevar el asunto a una instancia superior, según se requiera. ✓ Asegurarse de que todas las actividades de respuesta involucradas se registren adecuadamente para análisis posterior. ✓ Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo. ✓ Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente.	Oficina de Tecnología y Sistemas de Información	Informe de Gestión de Incidentes de Seguridad de la Información Soportes de ejecución de acciones. Planes de mitigación de vulnerabilidades ejecutados Registro del reporte del

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	✓ Una vez que el incidente se haya tratado lo suficiente, cerrarlo formalmente y hacer un registro de esto.		incidente - Aplicación Modulo de Incidentes de seguridad de la información
	Escalar los incidentes a niveles superiores o control interno en caso de que sea requerido.		Registro comunicación

4.1.5 Aprendizaje obtenido de los incidentes de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Usar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la posibilidad o el impacto de incidentes futuros	Documentar todos los incidentes de seguridad de la información reportados en el MEN.	Oficina de Tecnología y Sistemas de Información	Aplicación Modulo de Incidentes de seguridad de la información
	Llevar una bitácora de los incidentes de seguridad de la información reportados y atendidos en el MEN Por medio del aplicativo dispuesto para tal fin.		Aplicación Modulo de Incidentes de seguridad de la información

4.1.6 Recolección de evidencia

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	Desarrollar y seguir procedimientos internos cuando se trata con evidencia para propósitos de acciones legales y disciplinarias en el MEN.	Oficina de Tecnología y Sistemas de Información	Procedimientos y Documentación aplicable
	Tener en cuenta que los procedimientos para evidencia deben contener actividades tales como; identificación, recolección, adquisición y preservación de evidencia de acuerdo con los diferentes tipos de medios, dispositivos y estado de los dispositivos, por ejemplo, encendidos o apagados. Los procedimientos deben tener en cuenta: ○ La cadena de custodia; ○ La seguridad de la evidencia; ○ La seguridad del personal; ○ Los roles y responsabilidades del personal involucrado; ○ La competencia del personal; ○ La documentación; ○ Las sesiones informativas. ○ Para el transporte de elementos, se debe llevar la cadena de custodia.		Procedimientos y Documentación aplicable

5. Información de contacto

Cualquier inquietud relacionada con la guía política de gestión de incidentes de seguridad de la información, 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.16 Gestión de incidentes de seguridad de la información

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