Política de seguridad de la gestión de continuidad de negocio

Tabla de contenido

1 Objetivo

Asegurar que todos los aspectos relacionados con la seguridad de la información se incluyan en los planes de continuidad de negocio del MEN y así proteger la información.

2 Alcance

Esta política aplica para la definición del plan de continuidad de negocio y la recuperación en caso de desastres del MEN, en las cuales se deben incluir los requisitos de seguridad de la información.

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.
- **Continuidad de negocio:** Conjunto de actividades o procedimientos que facilitarán mantener el normal funcionamiento de la misionalidad de la entidad y la prestación de sus servicios.
- **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 Continuidad de la seguridad de la información

4.1.1 Planificación de la continuidad de la seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	Determinar si la continuación de la seguridad de la información se ha incluido dentro del proceso de gestión de continuidad de negocio o dentro del proceso de gestión para recuperación de desastres del MEN.	Oficina de Tecnología y Sistemas de Información	Procedimiento – gestión de disponibilidad Documentación asociada al Proceso Gestión de Servicios TIC
	Establecer los requisitos necesarios de seguridad de la información y la continuidad de la operación en caso de situaciones adversas, como desastres naturales o crisis, en el MEN.		Procedimiento – gestión de disponibilidad Plan de Gestión de Disponibilidad

4.1.2 Implementación de la continuidad de la seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La organización deberá establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Establecer, documentar, implementar y mantener: ○ Los controles de la seguridad de la información dentro de procesos de continuidad de negocio o recuperación de desastres, y sistemas y herramientas de apoyo. ○ Los cambios en los procesos, procedimientos e implementación, para mantener los controles de seguridad de la información existentes durante una situación adversa. Los controles de compensación para los controles de seguridad de la información que no se pueden mantener durante una situación adversa..	Oficina de Tecnología y Sistemas de Información	Documentación asociada al Proceso Gestión de Servicios TIC Procedimiento – gestión de disponibilidad Plan de Gestión de Disponibilidad
	Se debe contar con una estructura de gestión adecuada para prepararse, mitigar y responder a un evento perturbador usando personal con la autoridad, experiencia y competencia necesarias en el MEN.	La Alta Dirección del MEN (Comité Institucional de Gestión y Desempeño)	Formato Roles y Responsabilidades SGSI
	Nombrar personal de respuesta a incidentes con la responsabilidad, autoridad y competencia necesarias para manejar un incidente y mantener la seguridad de la información en el MEN.		Formato Roles y Responsabilidades SGSI
	Se deben desarrollar y aprobar planes, procedimientos de respuesta y recuperación documentados, en los que se especifique en detalle como el MEN gestionará un evento perturbador y mantendrá su seguridad de la información en un límite predeterminado, con base en los objetivos de continuidad de seguridad de la información definidos en el presente Manual.		Documentación asociada al Proceso Gestión de Servicios TIC Procedimiento – gestión de disponibilidad Plan de Gestión de Disponibilidad

4.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La organización deberá verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	Verificar a intervalos regulares, mínimo una vez al año, los controles de continuidad de la seguridad de la información establecidos e implementados en el MEN, con el fin de asegurar que son válidos y eficaces durante situaciones adversas. Se sugiere que se realice de la siguiente forma: ✓ Ejercitando y poniendo a prueba la funcionalidad de los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que son coherentes con los objetivos de continuidad de la seguridad de la información del MEN. ✓ Ejercitando y poniendo a prueba el conocimiento y las rutinas para operar los procesos, procedimientos y controles de continuidad de la seguridad de la información, para asegurar que su desempeño es coherente con los objetivos de continuidad de la seguridad de la información del MEN. ✓ Revisando la validez y la eficacia de las medidas de continuidad de la seguridad de la información cuando cambian los sistemas de información, los procesos, procedimientos y controles de seguridad de la información, o los procesos y soluciones de gestión de recuperación de desastres/gestión de continuidad de negocio del MEN.	Oficina de Tecnología y Sistemas de Información	Informes de verificación de la continuidad del negocio
	Establecer un plan de pruebas periódico, mínimo una vez al año, del plan de Contingencia de la Plataforma Tecnológica del MEN.		Informes de verificación de la continuidad del negocio

4.1.4 Disponibilidad de instalaciones de procesamiento de información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Implementar con redundancia suficiente las instalaciones de procesamiento de información para cumplir los requisitos de seguridad	Contar con un centro de datos alterno, para garantizar la disponibilidad de los servicios críticos del MEN, teniendo en cuenta las buenas prácticas de seguridad de la información establecidas en este documento.	Oficina de Tecnología y Sistemas de Información	Soportes contrato data center externo
	Identificar los requisitos del MEN para la disponibilidad de los sistemas de información. Cuando no se puede garantizar disponibilidad usando la arquitectura de los sistemas existentes, se deberían considerar componentes o arquitecturas redundantes.		Procedimiento – gestión de disponibilidad
	Probar cuando sea aplicable, los sistemas de información redundante del MEN para asegurar que la conexión automática de emergencia después de una falla de un componente a otro funcione de la forma prevista.		Informes de verificación de la continuidad del negocio

5. Información de contacto

Cualquier inquietud relacionada con la guía política de seguridad de la información en la continuidad de negocio, 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.17 Aspectos de seguridad de la información de la gestión de continuidad de negocio.

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 P	**Nombre**	Lina Mercedes Durán	**Nombre**	Roger Quirama
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