Política de seguridad en la relación con los proveedores

Tabla de contenido

1 Objetivo

Establecer las condiciones para la prestación de los servicios, responsabilidades y controles que ayuden a proteger la información involucrada en las relaciones entre el Ministerio de Educación Nacional con sus terceros, frente a interceptaciones, copia, modificación, divulgación y destrucción no autorizada, que puedan afectar los principios de integridad, disponibilidad y confidencialidad de la información.

2 Alcance

Esta guía política aplica para todos los proveedores que para la ejecución de su trabajo requieran acceder a la información o infraestructura tecnológica del Ministerio de Educación Nacional.

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.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- **Vulnerabilidad:** Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.
- **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 Seguridad de la información en las relaciones con los proveedores

4.1.1 Política de seguridad de la información para las relaciones con los proveedores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar la protección de los activos de información de la entidad que sean accesibles a los proveedores	Identificar y exigir los controles de seguridad de la información a tener en cuenta en el acceso de los proveedores a la información del MEN.	Subdirección de contratación Oficina de tecnología y sistemas de Información	Contratos Políticas SGSI
	Tener en cuenta los procesos y procedimientos que va a implementar el MEN, al igual que los procesos y procedimientos que debe exigir a sus proveedores que implementara, incluidos: ○ La identificación y documentación de los tipos de proveedores, por ejemplo, servicios de TI, utilidades logísticas, servicios financieros, componentes de la infraestructura de TI, a quienes el MEN permitirá acceso a su información. ○ Un proceso y un ciclo de vida normalizado para la gestión de las relaciones con los proveedores. ○ La definición de los tipos de acceso a la información que se permitirá a diferentes tipos de proveedores, y el seguimiento y el control del acceso. ○ Los requisitos mínimos de seguridad de la información para cada tipo de información y tipo de acceso, que sirvan como base para los acuerdos con proveedores individuales, con base en las necesidades y requisitos del negocio del MEN, y su perfil de riesgo.		Definición de roles y responsabilidades del SGSI Política control de acceso
	Definir los procesos y procedimientos para hacer seguimiento del cumplimiento de los requisitos de seguridad de la información establecidos para cada tipo de proveedor y tipo de acceso, incluida la revisión por una tercera parte y la validación del producto.	Subdirección de contratación Oficina de Tecnología y	Documentación asociada al proceso gestión de servicios TIC

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Identificar los tipos de obligaciones aplicables a los proveedores para proteger la información del MEN.	sistemas de Información	Contratos Acuerdos de confidencialidad
	Definir las condiciones bajo las cuales los requisitos y controles de seguridad de la información se documentarán en un acuerdo firmado por el MEN y los terceros (Proveedores).		Contratos Acuerdos de confidencialidad Política de transferencia de información
	Gestionar el manejo de incidentes y contingencias asociadas con el acceso de proveedores, incluidas las responsabilidades tanto del Ministerio de Educación Nacional como de los proveedores.	Oficina de tecnología y sistemas de Información Gestión Humana	Procedimiento Gestión de incidentes
	Brindar formación sobre toma de conciencia para el personal del MEN que interactúa con el personal de los proveedores, con respecto a las reglas apropiadas de interacción y comportamiento, con base en el tipo de proveedor, y en el nivel de acceso del proveedor a los sistemas e información del MEN.		Plan de sensibilización SGSI
	Gestionar las transiciones necesarias de información, instalaciones de procesamiento de información y cualquier otra cosa que sea necesario mover, y asegurar que la seguridad de la información se mantiene durante todo el período de transición.	Oficina de tecnología y sistemas de Información	Informes de gestión de seguridad informática e infraestructura

4.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar, o suministrar componentes de infraestructura de TI para la información de la entidad	Establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información del Ministerio de Educación Nacional.	Oficina de Tecnología y Sistemas de Información	Contratos
	Exigir que, en todos los contratos o acuerdos con terceras partes, que implique un intercambio, uso o procesamiento de información del MEN, se deben realizar acuerdos de confidencialidad y/o acuerdos de protección de datos sobre el manejo de la información.	Subdirección de contratación	Contratos Política de transferencia de información
	Incluir en los acuerdos de confidencialidad con los proveedores: • Descripción de la información que se va a suministrar o a la que se va a tener acceso, y los métodos para suministrar la información o para acceder a ella. • Clasificar la información de acuerdo con el esquema de clasificación del MEN. • Asegurar y describir que los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor se cumplan. • Acordar e implementar un grupo de controles que incluyan controles de acceso, revisión del desempeño, seguimiento, reporte y auditoría. • Definir las reglas de uso aceptable de la información, incluido el uso inaceptable, si es necesario. • Exigir una lista explícita de personal del proveedor autorizado para tener acceso a la información del MEN o recibirla de ella, o los procedimientos	Subdirección de contratación Oficina de Tecnología y sistemas de Información	Política de transferencia de información Acuerdo de confidencialidad

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	o condiciones para la autorización, y el retiro de la autorización para el acceso o recibo de información de la entidad por parte del personal del proveedor. • Exigir el derecho de auditar los procesos y controles de los proveedores, relacionados con el acuerdo. • Exigir que los proveedores entreguen periódicamente un informe independiente sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes presentados en el informe. • Monitorear las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.		

4.1.3 Cadena de suministro de tecnología de información y comunicación

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Incluir en los acuerdos con los proveedores los requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de	Asegurar que los acuerdos con proveedores incluyan requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	Oficina de Tecnología y Sistemas de Información	Especificaciones técnicas de los contratos Contratos
	Incluir los siguientes temas en los acuerdos de confidencialidad con los proveedores, concernientes a la seguridad de la cadena de suministro: • Definir los requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología de la información y de comunicaciones, además de los requisitos generales de seguridad de la información para las relaciones con los proveedores.		Especificaciones técnicas Contratos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	• Exigir para los servicios de tecnología de información y de comunicaciones, que los proveedores divulguen los requisitos de seguridad de la organización a lo largo de la cadena de suministro, si los proveedores contratan externamente partes del servicio de tecnología de la información y comunicaciones que suministran al MEN. • Exigir que los proveedores divulguen prácticas de seguridad adecuadas a lo largo de la cadena de suministro, para los productos de tecnología de información y comunicaciones, si estos productos incluyen componentes comprados a otros proveedores. • Implementar un proceso de seguimiento y métodos aceptables para validar que los productos y servicios de tecnología de información y comunicación cumplan los requisitos de seguridad establecidos. • Implementar un proceso para identificar los componentes de los productos o servicios que son críticos para mantener la funcionalidad, y, por tanto, requieren una mayor atención y escrutinio cuando se construyen por fuera del MEN, especialmente si el proveedor en el nivel superior contrata externamente aspectos de componentes de productos o servicios a otros proveedores. • Definir reglas para compartir información concerniente a la cadena de suministro y cualquier problema y compromisos entre el MEN y los proveedores. • Implementar procesos específicos para la gestión del ciclo de vida y la disponibilidad de componentes de tecnología de información y de comunicación, y de los riesgos de seguridad asociados. Esto incluye la gestión de riesgos de componentes que ya no están disponibles debido a que los proveedores ya no están en el negocio o ya no suministran estos componentes debido a que se han hecho avances en la tecnología.		

4.2 Gestión de la prestación de servicios de proveedores

4.2.1 Seguimiento y revisión de los servicios de los proveedores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	Hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores, que incluya: • Asegurar que los términos y condiciones de seguridad de la información de los acuerdos se cumplan, y que los incidentes y problemas de seguridad de la información se gestionan apropiadamente. • Definir un proceso de relacionamiento para la gestión del servicio entre la organización y el proveedor para: o Hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos. o Revisar los reportes de servicio elaborados por el proveedor, y concertar reuniones de avance regulares, según se exija en los acuerdos. o Llevar a cabo auditorías de los proveedores, junto con la revisión de reportes de auditores independientes, si están disponibles, y acciones sobre las cuestiones identificadas. o Suministrar información acerca de incidentes de seguridad de la información y revisar esta información según se exija en los acuerdos y en cualquier directriz y procedimiento de soporte. o Revisar los rastros de auditoría del proveedor, y los registros de eventos de seguridad de la información, problemas operacionales, fallas, rastreo de fallas e interrupciones relacionadas con el servicio entregado. o Resolver y gestionar cualquier problema identificado.	Oficina de Tecnología y Sistemas de Información	Informes de supervisión Procedimiento de gestión de incidentes

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Revisar los aspectos de seguridad de la información de las relaciones de los proveedores con sus propios proveedores. ○ Exigir que el proveedor mantenga una capacidad de servicio suficiente, junto con planes ejecutables destinados a asegurar que se mantienen los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre.		

4.1.3.2 Gestión de cambios en los servicios de los proveedores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.	Gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del MEN involucrados, y la revaloración de los riesgos de seguridad de la información. Debe considerar los siguientes aspectos: ○ Los cambios en los acuerdos con los proveedores; ○ Los cambios hechos por la organización para implementar: ○ Las mejoras a los servicios ofrecidos en la actualidad; ○ El desarrollo de nuevas aplicaciones y sistemas; ○ Las modificaciones o actualizaciones a las políticas y procedimientos de la entidad; ○ Los controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad.	Oficina de Tecnología y Sistemas de Información	Procedimiento gestión de cambios

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Los cambios en los servicios de los proveedores para implementar: o Cambios y mejoras en las redes. o El uso de nuevas tecnologías. o La adopción de nuevos productos o versiones/ediciones más recientes. o Nuevas herramientas y ambientes de desarrollo. o Cambios en las ubicaciones físicas de las instalaciones de servicio. o Cambio de proveedores. o Contratación externa de otros proveedores.		

5. Información de contacto

Cualquier inquietud relacionada con la política de seguridad en la relación con los proveedores, favor remitirla al correo seguridaddigital@mineducacion.edu.co

6. Revisión de la guía

Esta política debe ser revisada por la OTSI y la Subdirección de Contratación como mínimo una vez al año.

7. Referentes

7.1 Referentes Normativos

Norma ISO 27001
Dominio A.15 Relaciones con los proveedores

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