Guía Política Seguridad en la Nube

Tabla de contenido

1 Objetivo

Asegurar los aspectos a tener en cuenta para el aseguramiento de la información en la nube –Cloud. La correcta implementación de los servicios de información en la Nube de la Entidad reducirá el riesgo de que se presenten incidentes de seguridad que afecten la imagen de la entidad y generen un daño irreparable.

2 Alcance

Esta guía política aplica a todos los sistemas de información del MEN que se encuentren en plataformas en la nube, incluyendo los sistemas de información que se desean migrar o crear.

3 Definiciones

- **Integridad:** Propiedad de la información que consiste en 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 consiste en garantizar el acceso y uso de la información y los sistemas de tratamiento de esta a los individuos, entidades o procesos autorizados cuando lo requieran.
- **Confidencialidad:** Propiedad de la información que consiste en 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.
- **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.
- **Cloud Computing:** Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicado en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.
- **Clúster: Conjunto** de servidores que trabajan como una única maquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.
- **CPD:** Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

- **CRM:** “Customer Retationship Management”. Gestión de la Relación con el Cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.
- **Data Center:** Un centro de almacenaje de datos y que provee servicios de negocio que entrega de forma segura aplicaciones y datos a usuarios remotos a través de Internet.
- **ISO27001:** Estándar para la seguridad de la información. Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la metodología del Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar).
- **Multitenancy:** Uso común entre todos los clientes y usuarios de los servicios de computación en la nube desde la misma plataforma tecnológica del proveedor contratado.
- **On-demand**: Término referido al concepto de —bajo demanda. Dentro del ámbito tecnológico se utiliza para expresar la flexibilidad de los productos cloud, basados en un modelo de pago por uso y en los cuales el proveedor pone a disposición del cliente todos sus recursos, pudiéndolos usar bajo petición previa.
- **SLA:** “Service Level Agreement” o “Acuerdo de Nivel de Servicio”. Es un protocolo plasmado normalmente en un documento de carácter legal por el que una compañía que presta un servicio a otra se compromete a hacerlo bajo determinadas condiciones y con unas prestaciones mínimas.

4 Directrices

CONTROL	DIRECTRICES	ACTORES
Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	El estándar ISO 27017 internacional, proporciona directrices para la implementación de los controles de seguridad de la información en los servicios de la computación en la nube, los cuales deben ser tenidos en cuenta a la hora de contratar o usar estos dentro de la Entidad.	Oficina de tecnología y sistemas de información
	En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información del MEN, acceso a información personal, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información del Ministerio o personal.	
	No se deben utilizar servicios de computación en la nube cuyo análisis de riesgos indique niveles no tolerables para la protección de información de la Entidad. Los resultados del análisis y gestión riesgos deben ser determinantes para aceptar o rechazar la utilización de servicios de computación en la nube de pago o gratuitos.	
	Para almacenar información de datos personales, en los términos definidos por la ley 1266 de 2008 o 1581 de 2012, en servicios de almacenamiento en la nube fuera del territorio nacional se debe contar con la autorización del titular del dato personal.	
	En los contratos celebrados en Colombia con proveedores de servicios de computación en la nube, se debe incluir el cumplimiento de las políticas de seguridad de la información de la Entidad, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual vigentes sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.	
	Al contratar servicios de computación en la nube se debe contemplar y tratar los riesgos de pérdida de continuidad, disponibilidad e integridad por fallas en las plataformas de computación.	
	En los casos que se requiera el almacenamiento en la nube de información: clasificada como reservada, pública clasificada e información de carácter personal está debe permanecer cifrada para evitar su divulgación o acceso no autorizados. El cifrado se debe realizar de acuerdo con las políticas de seguridad de la información de la Entidad.	
	El uso de los servicios de computación en la nube dentro de la Entidad debe ser exclusivo para el cumplimiento de las funciones de las labores dentro de la Entidad, no está autorizado el uso de servicios de computación en la nube para fines personales.	

	Los siguientes lineamientos específicos se aplican de acuerdo con el tipo de servicio de computación en la nube: • En los servicios de correo electrónico se deben cumplir la política institucional de correo electrónico. • En los servicios de correo electrónico y almacenamiento en la nube se deben cumplir los límites de espacio de almacenamiento que determine el proceso de gestión de tecnologías de información. • Los archivos almacenados en las plataformas de nube se tendrán de acuerdo con los lineamientos que determinen las tablas de retención documental de cada proceso para sus respectivos registros electrónicos	
	Realizar monitoreo a los logs de trasferencia de datos hacia la nube.	Operador de Servicios TICs
	Los servicios de computo en la nube deben cumplir con los procedimientos de capacidad, disponibilidad, cambios y backup de la Entidad	
	Proteger los volúmenes a cualquier exposición	
	Realizar backup de la información que se envía hacia la nube	
	Los usuarios de administración de la plataforma deben mantener en estricta confidencialidad las contraseñas para acceso a los servicios de computación en la nube y el acceso a la plataforma debe ser con doble factor de autenticación.	
	Cualquier servicio de computación en la nube que requiera o se utilice cualquier proceso de la entidad debe ser aprobados por la Oficina de Tecnología y Sistemas de Información.	Procesos de MEN

5 Información de contacto

Cualquier inquietud relacionada con la Guía política de seguridad en la nube, favor remitirla al correo seguridaddigital@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
Dominios y controles de la norma.
Norma ISO 27017
Controles de seguridad para servicios en la nube.

7.1.1 Referentes de política nacional

Manual de seguridad y privacidad de la información – Min TIC - Estrategia de Gobierno Digital.

Guía 12 - Seguridad en la Nube

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	Debido a los cambios en las tecnologías que utiliza la Entidad se crea dicha política asociada al sistema de gestión de seguridad de la información.

Registro de aprobación					
Elaboró		**Revisó**		**Aprobó**	
Nombre	Edwar Hidalgo Acosta	**Nombre**	Lina Vannesa Perdomo	**Nombre**	Roger Quirama Garcia
Cargo	Contratista de la Oficina de Tecnología y Sistemas de Información	**Cargo**	Contratista Subdirección de Desarrollo Organizacional.	**Cargo**	Jefe de la Oficina de Tecnología y Sistemas de Información