Guía - Política de adquisición, desarrollo y mantenimiento de sistemas

Tabla de conten

Contenido

1 Objetivo 3
2 Alcance 3
3 Definiciones 3
4 Directrices 4
4.1 Requisitos de seguridad de los sistemas de información 4
4.1.1 Análisis y especificación de requisitos de seguridad de la información 4
4.1.2 Seguridad de servicios de las aplicaciones en redes públicas 8
4.1.3 Protección de transacciones de los servicios de las aplicaciones 10
5 Información de contacto 12
6 Revisión de la guía 12
7 Referentes 12
7.1 Referentes Normativos 12
7.1.1 Referentes de política nacional 12
7.1.2 Referentes de políticas del MEN 12

1 Objetivo

Asegurar que la seguridad digital sea una parte integral de los sistemas de información del MEN durante todo el ciclo de vida.

2 Alcance

Esta guía política aplica a todos los sistemas de información del MEN, incluyendo los sistemas de información que prestan servicios sobre redes públicas.

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.
- **Criptografía:** Es la ciencia que estudia la transformación de la información mediante algoritmos, protocolos y sistemas con el fin de protegerla y dotar de seguridad a las comunicaciones y a las entidades que se comunican.
- **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.

4 Directrices

4.1 Requisitos de seguridad de los sistemas de información

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información del MEN durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.

4.1.1 Análisis y especificación de requisitos de seguridad de la información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
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.	Apoyar a todas las áreas del MEN en la adquisición o mejora de aplicativos o software.	Oficina de tecnología y sistemas de información	ST-PR-11 Procedimiento Gestión de Proyectos ST-PR-12 Procedimiento Gestión de Cambios
	Identificar los requisitos de seguridad de la información usando varios métodos y promover que los terceros (Operador TI, Aplicaciones, Fábrica de software, seguridad informática etc.) los cumplan: ✓ Las políticas de seguridad de la información y demás reglamentación definida por el MEN. ✓ Identificación de amenazas de seguridad de la información. ✓ Revisiones de incidentes, o uso de umbrales de vulnerabilidad.	Oficina de tecnología y sistemas de información Operador de TI (Aplicaciones, Fábrica de software, seguridad informática)	Manual de Seguridad Digital y Guías de Política. Plan de comunicaciones y sensibilización del SGSI
	Documentar y revisar los resultados de la identificación de los requisitos de seguridad de la información por todas las partes interesadas (OTSI, Operador TI, Aplicaciones, Fábrica de software, seguridad etc.).	Oficina de tecnología y sistemas de información Operador de TI (Aplicaciones, Fábrica de software,	Diagnóstico del MSPI y plan de cierre de brechas.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
		seguridad informática)	
	Integrar en la etapa de diseño de los proyectos de sistemas de información la identificación y gestión de los requisitos de seguridad de la información y los procesos asociados.	Operador de TI (Aplicaciones, Fábrica de software, seguridad informática)	Documentación de los proyectos de sistemas de información.
	Exigir, para nuevos desarrollos o mejoras en los sistemas de información existentes, las mejores prácticas en el ciclo de vida desarrollo de software SDLC, entre los cuales están: **1. Fase de requerimientos:** ✓ Controles de autenticación y sesión, Los requisitos derivados de los procesos y políticas del MEN, tales como los requisitos de ingreso y seguimiento, y de no repudio. Los requisitos de autenticación de usuario (Usuarios, Claves). Los requisitos para la entrega a producción de servicios tecnológicos. Manejo adecuado de sesiones ✓ Control de roles y privilegios Los procesos para conceder acceso y autorización a los usuarios del MEN, al igual que a los usuarios privilegiados (Administradores, súper usuarios o técnicos) mediante la definición de la matriz de roles y privilegios. Informar a los usuarios y operadores sobre sus deberes y responsabilidades. Asegurar la asignación de menor privilegio, los usuarios solo deben ser capaces de acceder a los sistemas de información, que por el desempeño de sus funciones requieran. ✓ Requerimientos orientados al riesgo Las necesidades de protección de activos de información involucrados, para	Oficina de tecnología y sistemas de información	Manual de Seguridad Digital y Guías de Política. Protocolo de ciclo de vida del software. Listas de chequeo de verificación de las fases del desarrollo y mantenimiento de software. ST-PT-01 - Protocolo de paso a producción para la entrega en productivo de nuevas soluciones tecnológicas.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	preservar la disponibilidad, confidencialidad e integridad; Los requisitos exigidos por otros controles de seguridad, por ejemplo, interfaces con el ingreso o seguimiento, o los sistemas de detección de fuga de datos. ✓ Aprobación de privilegios **2. Fase de análisis y diseño:** ✓ Acceso a componentes y a la administración del sistema. ✓ Pistas de auditoría ✓ Gestión de sesiones ✓ Datos históricos. ✓ Manejo apropiado de errores ✓ Separación de funciones (Segregación de funciones) **3. Fase de implementación y codificación:** ✓ Aseguramiento del ambiente de desarrollo ✓ Elaboración de documentación técnica ✓ Codificación segura (Buenas prácticas) o Validación de entradas o Codificación de salidas y versiones. o Estilo de programación o Manejo de log de cambios. o Prácticas criptográficas o Manejo de errores y logs o Manejo de archivos. o Manejo de memoria. o Estandarización y reutilización de funciones de seguridad ✓ Seguridad en las comunicaciones ✓ Seguridad en el paso a ambientes de producción		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	4. Fase de pruebas ✓ Control de calidad en controles de seguridad (con y sin credenciales de acceso) ✓ Realizar pruebas de código seguro ✓ Comprobación de gestión de configuraciones. ✓ Caja blanca y caja negra ✓ Pruebas de top ten de OWASP ✓ Pruebas de Fuzzing **5. Fase de mantenimiento.** ✓ Aseguramiento basado en RIESGOS. ✓ Pruebas de seguridad (Caja blanca y caja negra) después de los cambios. ✓ Crear plan de respuesta a incidentes (para identificar nuevas amenazas)		

4.1.2 Seguridad de servicios de las aplicaciones en redes públicas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	Exigir a los proveedores y operadores TIC que la información del MEN involucrada en los servicios de aplicaciones que pasan sobre redes públicas se protejan de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.	Oficina de tecnología y sistemas de información	Contratos con los proveedores. Informes de ejecución de los contratos con los proveedores
	Exigir a los proveedores y operadores TIC que incluyan las siguientes consideraciones de seguridad de la información para servicios de aplicaciones que están soportadas sobre redes públicas: ✓ El nivel de confianza que cada parte requiere con relación a la identidad declarada por la otra parte, por ejemplo, por medio de autenticación (Mecanismos de autenticación). ✓ Los procesos de autorización asociados a quién puede aprobar el contenido o expedir o firmar documentos transaccionales clave. ✓ Los mecanismos para que los aliados de servicios de comunicación estén completamente informados de sus autorizaciones para suministro o uso del servicio. ✓ Los requisitos para confidencialidad, integridad, prueba de despacho y recibo de documentos clave y el no repudio de los contratos, por ejemplo, asociados con procesos de ofertas y contratos, y los mecanismos para su cumplimiento. ✓ El nivel de confianza requerido en la integridad de los documentos clave. ✓ Los requisitos de protección de cualquier información, especialmente la confidencial.		Contratos con los proveedores. Informes de ejecución de los contratos con los proveedores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	✓ La confidencialidad e integridad de cualquier transacción de pedidos, información de pagos, detalles de la dirección de entrega y confirmación de recibos. ✓ El grado de verificación apropiado de la información de pago suministrada por un cliente. ✓ La selección de la forma de arreglo de pago más apropiado para protegerse contra fraude. ✓ El nivel de protección requerido para mantener la confidencialidad e integridad de la información del pedido; ✓ Los mecanismos para evitar la pérdida o duplicación de información de la transacción. ✓ La responsabilidad civil asociada con cualquier transacción fraudulenta. ✓ Los requisitos de seguros.		

4.1.3 Protección de transacciones de los servicios de las aplicaciones

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	Brindar mecanismos (SFTP, VPN, Base de datos de pruebas) para que la información del MEN involucrada en las transacciones de los servicios de las aplicaciones se proteja para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción no autorizada de mensajes.	Oficina de tecnología y sistemas de información	Solicitudes mesa de ayuda de tecnología. SFTP VPN Base de datos de pruebas.
	Exigir al operador de TI (Aplicaciones, Seguridad) que incluyan las consideraciones de seguridad de la información para las transacciones de los servicios de las aplicaciones, entre otras: o El uso de firmas electrónicas por parte de cada una de las partes involucradas en la transacción; o Todos los aspectos de la transacción, es decir, asegurar que: • La información de autenticación secreta de usuario, de todas las partes, se valide y verifique. • La transacción permanezca confidencial. Se mantenga la privacidad asociada con todas las partes involucradas. • La trayectoria de las comunicaciones entre todas las partes involucradas esté cifrada. • Los protocolos usados para comunicarse entre todas las partes involucradas sean seguros. • El almacenamiento de los detalles de la transacción se realice en un entorno que no sea accesible públicamente, por ejemplo, en una plataforma de almacenamiento existente en la intranet del		Contratos con el operador de TI y con la fábrica de software Informes de ejecución del contrato con el operador TI y con la fábrica de software

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	MEN, y no sea retenido ni expuesto en un medio de almacenamiento accesible directamente desde Internet. • Que en donde se use una autoridad confiable (por ejemplo, para los propósitos de emitir y mantener firmas o certificados digitales), la seguridad esté integrada e incluida en todo el proceso de gestión de certificados/firmas de un extremo a otro.		

5 Información de contacto

Cualquier inquietud relacionada con la Guía política de adquisición, desarrollo y mantenimiento de sistemas, 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
- Dominio A.14 Adquisición, desarrollo y mantenimiento de sistemas.

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 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	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