Guía - Política Seguridad de las operaciones

Tabla de contenido

1 Objetivo

Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información del MEN.

2 Alcance

Esta guía de política de seguridad de las operaciones aplica para la OTSI del MEN, quienes deben preparar procedimientos documentados para las actividades operacionales asociadas con las instalaciones de procesamiento y comunicación, tales como los procedimientos de encendido y apagado, copias de respaldo, mantenimiento de equipos, manejo de medios, salas de informática y gestión y seguridad del manejo de correo.

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 MEN es considerado importante o de alta validez para el mismo, 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.

- **MEN:** Ministerio de Educación Nacional
- **Mesa de Ayuda de Tecnología:** Centro de Atención al Usuario mediante el cual la OTSI presta servicios para gestionar y atender de requerimientos relacionados con los servicios TIC en el MEN.
- **OneDrive:** Plataforma en la nube de Microsoft que permite guardar los archivos o documentos (Ejemplo: información pública de las áreas del MEN) en línea y acceder a ellos desde cualquier lugar o equipo con conexión a Internet.
- **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.
- **Correo electrónico institucional:** Es el servicio de correo que le asigna el Ministerio a cada colaborador para que lo utilice en el desarrollo de sus funciones.

4. Directrices

4.1 Procedimientos operacionales y responsabilidades

4.1.1 Procedimientos de operación documentados.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten	Documentar, actualizar, publicar y socializar los procedimientos de operación.	Oficina de Tecnología y Sistemas de Información	Procedimientos de la operación publicados en el SIG, proceso de Gestión de Servicios TIC

4.1.2 Gestión de cambios

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Efectuar todos los cambios a la infraestructura informática y/o servicios de acuerdo con los lineamientos internos.	Oficina de Tecnología y Sistemas de Información	Procedimiento Gestión de Cambios (ST-PR-12) Instructivo Lineamientos Gestión de Cambios (ST-IN-03) del Proceso de Gestión de servicios TIC.
	Llevar una trazabilidad de cambios solicitados y gestionados.		Mesa de ayuda te tecnología. Informe de RFC gestionados.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Especificar en el procedimiento de Gestión de Cambios los canales autorizados para la recepción de solicitudes de cambios.		Procedimiento Gestión de Cambios (ST-PR-12) Mesa de ayuda te tecnología.
	Especificar en qué momento existen cambios de emergencia en la cual se debe asegurar que los cambios se apliquen de forma rápida y controlada.		Procedimiento Gestión de Cambios (ST-PR-12)
	Planear los cambios sobre sistemas de información para asegurar que se cuentan con todas las condiciones requeridas para ejecutarlos de una forma exitosa y se debe involucrar e informar a los colaboradores o terceros que por sus funciones tienen relación con el sistema de información.		Calendario de cambios. Soporte de cierre de la solicitud.
	Evaluar los impactos potenciales que podría generar un cambio a la aplicación previo a su aplicación, incluyendo aspectos funcionales y de seguridad de la información, estos impactos se deben considerar en la etapa de planificación del cambio para poder identificar acciones que reduzcan o eliminen el impacto.		Formato de Requerimientos de cambio ST-FT-07
	Probar los cambios realizados sobre sistemas de información para asegurar que se mantiene operativo el sistema de información, incluyendo aquellos aspectos de seguridad de la información del sistema y que el propósito del cambio se cumplió satisfactoriamente.		Soportes de revisión del éxito de la ejecución del cambio. PIR (Revisión post implementación)
	Establecer y aplicar el procedimiento formal para la aprobación de cambios sobre sistemas de información existentes, como actualizaciones, aplicación de parches o cualquier otro cambio asociado a la funcionalidad de los sistemas de información y componentes que los soportan, tales como el sistema operativo o cambios en hardware.		Procedimiento Gestión de Cambios (ST-PR-12)
	Disponer de un plan de roll-back en la aplicación de cambios, que incluyan las actividades a seguir para abortar los cambios y volver al estado anterior.		Formato de Requerimientos de cambio ST-FT-07

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Realizar solicitudes de cambio en los servicios de infraestructura y sistemas de información del Ministerio de acuerdo con lo establecido en los procedimientos, con el fin de asegurar la planeación del cambio y evitar una afectación a la disponibilidad, integridad o confidencialidad de la información.	Todos los colaboradores y terceros del MEN	Mesa de ayuda de tecnología.

4.1.3 Gestión de capacidad

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.	Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (capacity planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica del MEN. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.	Oficina de Tecnología y Sistemas de Información	- Plan de Capacidad (ST-PL-02). - Procedimiento Gestión de Capacidad (ST-PR-03)

4.1.4 Separación de los ambientes de desarrollo, pruebas y operación.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	Proveer los recursos necesarios que permitan la separación de ambientes de pruebas, certificación y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes en el MEN.	Oficina de Tecnología y Sistemas de Información	Soportes de la ejecución de los controles.
	Establecer y mantener ambientes separados de pruebas, certificación y producción, dentro de la infraestructura de desarrollo de sistemas de información del MEN.		Servidores físicos, hipercongencia y Vblock.
	Seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (certificación, pruebas y producción), donde se establecen las condiciones a seguir para alcanzar la puesta en producción de un sistema nuevo o la aplicación de un cambio a uno existente.		Procedimiento Gestión de Cambios (ST-PR-12). ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas
	No se deben realizar pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción. Esto puede conducir a fraude o inserción de código malicioso.		Procedimiento Gestión de Cambios (ST-PR-12).
	No se deben utilizar datos reales del ambiente de producción, en los ambientes de desarrollo y pruebas sin antes haber pasado por un proceso de ofuscamiento.		Procedimiento Gestión de Cambios (ST-PR-12).
	Utilizar controles de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.		Directorio activo.
	Identificar claramente las interfaces de los sistemas para poder determinar a q instancia se está realizando la conexión.		Nomenclatura definida para identificar los ambientes y las interfaces.
	Identificar claramente los ambientes, para evitar así confusiones en la aplicación de tareas o en la ejecución de procesos propios de cada uno.		Nomenclatura definida para identificar los ambientes.
	Informar y consultar con el(los) proceso (s) o dependencias propietario(s) de la información los cambios a sistemas en producción que involucren aspectos funcionales.		Procedimiento Gestión de Cambios (ST-PR-12).

4.2 Protección contra códigos maliciosos

4.2.1 Controles contra códigos maliciosos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	Asegurar que la infraestructura de procesamiento de información del MEN, cuente con un sistema de detección y prevención de intrusos, herramienta de Anti-Spam y sistemas de control de navegación, con el fin de asegurar que no se ejecuten virus o códigos maliciosos.	Oficina de tecnología y sistemas de información	Consola antivirus.
	Restringir la ejecución de aplicaciones y mantener instalado y actualizado el antivirus, en todas las estaciones de trabajo y servidores del MEN, de manera que se reduzca el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica del MEN y los servicios que se ejecutan en la misma.		Consola antivirus.
	Administrar el antivirus para proteger a nivel de red y de estaciones de trabajo del MEN, contra virus y código malicioso.		Consola antivirus.
	Asegurar que los equipos de terceros que son autorizados para conectarse a la red de datos del MEN tengan antivirus y cuenten con las medidas de seguridad apropiadas.		Mesa de ayuda de tecnología.
	Monitorear y supervisar todos los equipos conectados a la red del MEN.		Herramienta de monitoreo de los equipos conectados a la red.
	Monitorear las comunicaciones y/o la información que se generen, comuniquen, transmitan o trasporten y almacenen en cualquier medio, en busca de virus o código malicioso. Si se identifica virus o código malicioso y este no puede ser eliminado, la información será borrada.		Firewall
	Mantener actualizado a sus últimas versiones funcionales las herramientas de seguridad, incluido, motores de detección, bases de datos de firmas, software de gestión del lado cliente y del servidor, etc.		Plan de actualizaciones. Monitoreo periódico de actualizaciones. .
	Hacer revisiones y análisis periódicos del uso de software no malicioso en las estaciones de trabajo y servidores. La actividad debe ser programada de forma		Consola antivirus.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	automática.		
	Generar contraseñas robustas para las Bases de Datos, Red y Sistemas de Información.		Políticas de contraseñas del directorio activo.
	Contar con controles para analizar, detectar y restringir el software malicioso que provenga de descargas de sitios web de baja reputación, archivos almacenados en medios de almacenamiento removibles, código móvil, contenido de correo electrónico, etc.		Consola antivirus.
	Implementar soluciones lógicas (antivirus) y físicas (dispositivos perimetrales) que garanticen la protección de la información del MEN de posibles ataques internos o externos y que impidan el acceso no autorizado a la red del MEN las cuales deben permitir: Lógicas: ○ Detección de ataques en el momento que están ocurriendo o poco después. ○ Automatización de la búsqueda de nuevos patrones de ataque, con herramientas estadísticas de búsqueda y al análisis de tráfico anómalo. ○ Monitorización y análisis de las actividades de los usuarios en busca de elementos anómalos. ○ Auditoría de configuraciones y vulnerabilidades de los sistemas de IDS. ○ Descubrir sistemas con servicios habilitados que no deberían de tener, mediante el análisis del tráfico y de los logs. ○ Análisis de comportamiento anormal. Si se detecta una conexión fuera de hora, reintentos de conexión fallidos y otros, existe la posibilidad de que se esté en presencia de una intrusión. ○ Un análisis detallado del tráfico y los logs puede revelar una máquina comprometida o un usuario con su contraseña al descubierto. ○ Automatizar tareas como la actualización de reglas, la obtención y análisis de logs, la configuración de cortafuegos. Perimetrales:		Consola antivirus. Dispositivos perimetrales

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	○ Rechazar conexiones a servicios comprometidos. ○ Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https). ○ Proporcionar un único punto de interconexión con el exterior. ○ Redirigir el tráfico entrante a los dispositivos de seguridad con que cuenta el MEN. ○ Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde Internet. ○ Auditar el tráfico entre el exterior y el interior. ○ Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.		
	Asegurar que la Red del MEN sólo pueda acceder a los parámetros que el Firewall tenga permitido o posibilite mediante su configuración.		Firewall
	Configurar el software base y asignar las claves a los usuarios que lo soliciten.		Mesa de ayuda de tecnología.
	Llevar a cabo actividades o estrategias de sensibilización a los colaboradores y terceros del MEN, con el fin de generar una cultura de seguridad de la información, incluyendo la apropiación sobre la protección contra códigos maliciosos		Soportes de sensibilización.
	Asignar el único servicio de antivirus autorizado en el MEN, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques de virus, spyware y otro tipo de software malicioso. Además, este servicio tiene diferentes procesos de actualización que se aplican de manera periódica y segura. (Solo puede ser instalado por el personal de la OTSI)		Consola antivirus. Mesa de ayuda de tecnología.
	Asegurar que los colaboradores y terceros del MEN tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y asegurar que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.		Consola de antivirus. Políticas de accesos del directorio activo
	Realizar en cualquier momento un análisis bajo demanda a través del antivirus de cualquier archivo o repositorio que consideren sospechoso de contener software malicioso. En cualquier caso, los colaboradores y terceros cuando sea	Todos los colaboradores y	N/A

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	necesario siempre podrán consultar a la OTSI sobre el tratamiento que debe darse en caso de sospecha de malware.	terceros del MEN	
	Manejar el antivirus para analizar, verificar y (si es posible) eliminar virus o código malicioso de la red, el computador, los dispositivos de almacenamiento fijos, removibles, archivos, correo electrónico que estén utilizando para el desempeño de sus funciones laborales.		N/A
	No podrán desactivar o eliminar la suite de productos de seguridad, incluidos los programas antivirus o de detección de código malicioso, en los equipos o sistemas asignados para el desempeño de sus funciones laborales.		N/A
	Verificar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.		N/A
	Notificar si sospechan o detectan alguna infección por software malicioso, deben notificar a la mesa de ayuda de tecnología, para que, a través de ella, la OTSI tome las medidas de control correspondientes.		Mesa de ayuda de tecnología
	Destruir los archivos o mensajes, que le haya sido enviado por cualquier medio provisto por MEN, cuyo origen le sea desconocido o sospechoso y asume la responsabilidad de las consecuencias que puede ocasionar su apertura o ejecución. En estos casos no se deben contestar dichos mensajes, ni abrir los archivos adjuntos, el usuario debe reenviar el correo a la cuenta establecida para ello.		N/A

4.3 Copias de respaldo

4.3.1 Respaldo de información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.	Definir un procedimiento formal de administración y control de copias de respaldos que permita conocer qué información está respaldada y almacenada en las bóvedas de seguridad del sitio externo.	Oficina de Tecnología y Sistemas de Información	Documento de Políticas de Back Up
	Disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información.		Plan de Capacidad ST-PL-02
	Configurar la herramienta de ejecución de copias de respaldo para que automáticamente registre el éxito o errores en la ejecución.		Informe de la ejecución de copias de respaldo.
	Establecer un esquema de rotulado de las copias de respaldo, que contengan toda la información necesaria para identificar cada una de ellas y administrarlas debidamente.		Rótulos.
	Realizar periódicamente un análisis de las necesidades del negocio para determinar la información crítica que debe ser respaldada y la frecuencia con que se debe realizar.		Actas de reuniones de Gestión Técnica del Grupo de Infraestructura. Actas de Comité de Control de Cambios.
	Verificar periódicamente, la integridad de las copias de respaldo que se están almacenando, con el fin de preservar la integridad y disponibilidad de la información.		Informe de Plan de Recuperación.
	Definir un el procedimiento de reemplazo de los medios de almacenamiento de copias de respaldo, una vez terminada la posibilidad de ser reutilizados de acuerdo con lo indicado por el proveedor, y asegurar la destrucción de los medios de información retirados o desechados.		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Determinar junto a los propietarios de la información (Directores, Lideres, Coordinadores de áreas) los requerimientos para respaldar la información y los datos en función de su criticidad, para lo cual se debe elaborar y mantener el inventario de activos de Información del MEN.		Matriz de activos de la información en el módulo del SGSI-SIG y Documento de Políticas de Buck Up
	Disponer y controlar la ejecución de las copias, así como la prueba periódica de su restauración. Para esto se debe contar con instalaciones de respaldo que garanticen la disponibilidad de toda la información y del software crítico del MEN.		Informe de la ejecución de copias de respaldo.
	Efectuar las copias de información de los servidores, cada vez que se realice un cambio significativo en los sistemas operativos o configuraciones básicas.		Actas de Comité de Control de Cambios.
	Mantener siempre una copia de la información de los servidores, por lo menos con una antigüedad no superior a 24 horas.		Copia de respaldo incremental diaria.
	Realizar un respaldo diferencial semanalmente de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, desarrollo y dispositivos de red.		Copia de respaldo full semanal
	Realizar un respaldo full mensual de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, desarrollo y dispositivos de red.		Copia de respaldo full mensual
	Realizar respaldo full anual de los servidores de base de datos, servidores web, sistemas de información, aplicaciones, desarrollo y dispositivos de red.		Copia de respaldo full anual
	Mantener un monitoreo frecuente sobre la base de datos para así asegurar la integridad de la información respaldada.		Informe de monitoreo de la base de datos.
	Probar los procedimientos de restauración, para asegurar que son efectivos, que pueden ser ejecutados en los tiempos establecidos y que la información estará disponible en el evento que se requiera para su utilización en casos de emergencia.		Plan de restauración de copias de respaldo.
	Actualizar periódicamente las configuraciones de los servidores para la correcta ejecución de las copias de respaldo.		Actas de reuniones de Gestión Técnica del

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
			Grupo de Infraestructura
	Almacenar en una ubicación remota o externa las copias de respaldo recientes de información, junto con registros completos de las mismas y sus procedimientos documentados de restauración. • El sitio alterno donde se almacenan las copias de respaldo debe contar con los controles de seguridad necesarios, para cumplir con las medidas de protección y seguridad física apropiados. • Conservar los medios de almacenamiento de información en un ambiente que cuente con las especificaciones emitidas por los fabricantes o proveedores. • Las cintas de backup con la información actualizada, no deben permanecer más de una semana fuera del sitio externo.		Condiciones establecidas en el Contrato del Operador de Prestación de Servicios TIC.
	Contar con un responsable para: o Llevar el registro de los respaldos de información. o Registro del retiro de las cintas de backup del sitio externo. o Registro del ingreso de las cintas de backup al sitio externo. o Inventario de cintas de Backup. o Comprobación de Integridad de la Información		Contrato del Operador de Prestación de Servicios TIC.
	Retener los activos de información del MEN de acuerdo con las políticas de Buck Up y con lo establecido en las TRD.		Documento de Políticas de Buck Up y TRD.
	Realizar las copias de respaldo en horario no hábil, lo cual será verificado a través de procesos automáticos.		Informe de la ejecución de copias de respaldo.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Retirar la cinta de copias de seguridad del robot de cintas una vez se verifique la correcta ejecución de las copias de respaldo.		Soporte de etiquetado
	El dueño de los activos de información es responsable de definir claramente el periodo de retención de respaldos.	Líderes de procesos y Jefes de dependencias.	Documento de Políticas de Back Up y TRD.

4.3.1.2 Respaldo de información para usuarios finales

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información	Realizar los respaldos de información personal almacenada en los equipos asignados.	Todos los colaboradores y terceros del MEN.	N/A
	Almacenar toda la información relevante a sus funciones en el OneDrive suministrado por la OTSI.		One Drive
	Ningún colaborador del MEN puede realizar copias de respaldo en sus dispositivos de almacenamiento removibles personales, ya que esto puede ser denominado fuga de información.		N/A
	Dar estricto cumplimiento a esta política, dado que estaría sujeto a las acciones correspondientes.		N/A
	Almacenar la información crítica asociada con su labor en el servidor de archivos establecido para asegurar que la información está siendo respaldada.		Share point, NAS

4.4 Registro y seguimiento

4.4.1 Registro de eventos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información	Configurar la infraestructura, servidores, sistemas, bases de datos, para que queden registrados todos los accesos de los colaboradores del MEN a los sistemas, redes de datos y aplicaciones del Ministerio.	Oficina de tecnología y sistemas de información	Logs de infraestructura, servidores, sistemas y bases de datos. Procedimiento de Gestión de Eventos
	Habilitar los logs de eventos requeridos y estos deben ser revisados con regularidad.		Logs de infraestructura, servidores, sistemas y bases de datos.
	Hacer copia de respaldo de información de los eventos de auditoria, ya que en caso de un incidente de seguridad de la información deben estar disponibles.		Copias de respaldo de logs.

4.4.2 Protección de la información de registro

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado	Proteger las instalaciones y la información de registro contra alteración y acceso no autorizado.	Oficina de tecnología y sistemas de información	Sistema de Control de Acceso Físico. Controles de acceso a infraestructura, sistemas, servidores.
	Asegurar que los controles estén dirigidos a proteger contra cambios no autorizados de la información del registro y contra problemas con la instalación de registro, inclusive: a) alteraciones a los tipos de mensaje que se registran; b) archivos log que son editados o eliminados; c) se excede la capacidad de almacenamiento del medio de archivo log, lo que da como resultado falla en el registro de eventos, o sobreescritura de eventos pasados registrados.		Herramienta de monitoreo de la operación.
	Guardar en el archivo permanente algunos logs de auditoría, como parte de la política de retención de registros o debido a requisitos acerca de recolectar y retener evidencia.		Copias de respaldo de logs.

4.4.3 Registro del administrador y del operador

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.	Registrar todas las actividades de operación realizadas por los administradores de la infraestructura de procesamiento de información del MEN.	Oficina de Tecnología y Sistemas de Información	Logs de infraestructura, servidores, sistemas y bases de datos.
	Los administradores de la infraestructura tecnológica y de procesamiento de información del MEN deben tener asignada una cuenta de usuario exclusiva, a través de la cual se realizarán las actividades de administración y debe ser entregada a través de un proceso formal.		Cuentas de administración del directorio activo. Actas de entregas de usuarios de administración.

4.4.4 Sincronización de relojes

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia	Garantizar que todos los relojes de la infraestructura de procesamiento de información del MEN estén sincronizados con la hora legal colombiana.	Oficina de tecnología y sistemas de información	Configuración de infraestructura Servidor de sincronización de relojes.

4.5 Control de software operacional

4.5.1 Instalación de software en sistemas operativos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.	Verificar la instalación, configuración e implementación de seguridad, en los servidores conectados a la Red.	Oficina de Tecnología y Sistemas de Información	Servidor de dominio.
	Instalar y/o configurar todos los servidores conectados a la Red por medio del Operador de servicios TICs.		Comités de Cambio Informe de Cambios.
	Asegurar que las normas para el uso de los recursos del sistema y de la red, principalmente la restricción de directorios, permisos y programas a ser ejecutados por los usuarios sean aplicadas durante la configuración de los servidores.		Servidor de dominio.
	Asegurar que los servidores que proporcionen servicios a través de la red e internet: ○ Funcionen 24 horas del día los 365 días del año. ○ Reciban mantenimiento preventivo mínimo dos veces al año ○ Reciban mantenimiento semestral que incluya depuración de logs. ○ Reciban mantenimiento anual que incluya la revisión de su configuración. ○ Sean monitoreados por el Operador de Servicios TICs.		Contrato del operador de servicios TIC
	Configurar los servicios hacia internet sólo a través de los servidores autorizados por la OTSI.		Mesa de ayuda de tecnología. Formato de configuración de políticas de firewall ST-FT-03

4.6. Gestión de la vulnerabilidad técnica

4.6.1. Gestión de las vulnerabilidades técnicas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado	Realizar mínimo una vez al año una revisión de vulnerabilidades técnicas a los sistemas de información críticos y misionales por medio de ethical hacking y/o pruebas de penetración.	Oficina de Tecnología y Sistemas de Información	N/A
	Documentar, informar, gestionar y corregir las vulnerabilidades encontradas, adoptando acciones correctivas para mitigar los hallazgos, minimizar el nivel de riesgo y reducir el impacto.		
	Definir y establecer los roles y responsabilidades asociados con la gestión de la vulnerabilidad técnica, incluido el seguimiento de la vulnerabilidad, la valoración de riesgos de vulnerabilidad, las pruebas de gestión, la aplicación de parches, el seguimiento de activos y cualquier responsabilidad de coordinación requerida.		

4.6.2. Restricciones sobre la instalación de software

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.	Probar y evaluar la aplicación de actualizaciones antes de su instalación y valorar los riesgos asociados, para asegurar que son eficaces y no producen efectos secundarios.	Oficina de Tecnología y Sistemas de Información	N/A
	Restringir a los usuarios finales la instalación de software en los equipos del Ministerio.		
	Establecer y monitorear que la infraestructura tecnológica sea usada exclusivamente para el desempeño laboral, o para el desarrollo de las funciones, actividades y obligaciones acordadas o contratadas.		
	Controlar la instalación y uso de máquinas virtuales y sólo podrá realizarse siempre y cuando sea una necesidad para el uso de las funciones o labor contratada y no viole los derechos de autor.		
	Realizar de manera periódica una inspección del software instalado en los equipos del Ministerio y debe desinstalar el software no autorizado.		
	La OTSI a través de la Mesa de Servicios es la responsable de instalar, configurar y dar soporte a los equipos del Ministerio.		
	La OTSI es la dependencia autorizada para la administración del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales y comerciales		
	Sólo está permitido el uso de software licenciado por el Ministerio y/o aquel que sin requerir licencia de uso comercial sea expresamente autorizado por la Oficina de Tecnologías de la Información	Todos los colaboradores y terceros del MEN.	N/A
	Las aplicaciones generadas por el Ministerio en desarrollo de su misión institucional deben ser reportadas a la Oficina de Tecnologías de la Información para su administración.		

4.7. Consideraciones sobre auditorias de sistemas de información

4.7.1 Información controles de auditorías de sistemas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	Acordar y planificar cuidadosamente los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos del MEN para minimizar las interrupciones en los procesos del MEN.	Oficina de tecnología y sistemas de información	N/A
	Acordar con los líderes funcionales los requisitos de auditoría para acceso a sistemas y a datos.		
	Acordar y controlar el alcance de las pruebas técnicas de auditoría.		
	Limitar a acceso a software y datos únicamente para lectura en las pruebas de auditoría.		
	Prever el acceso diferente al de solo lectura solamente para copias aisladas de los archivos del sistema.		
	Borrar una vez que la auditoría haya finalizado, o se debería proporcionar información apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría.		
	Identificar y acordar los requisitos para procesos especiales y adicionales.		
	Realizar fuera de horas laborales las pruebas de auditoría que puedan afectar la disponibilidad del sistema.		
	Hacer seguimiento de todos los accesos y logged para producir un rastro de referencia.		

5. Información de contacto

Cualquier inquietud relacionada con la Guía política seguridad de las operaciones, 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.12 Seguridad de las operaciones

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