Guía - Política de Uso adecuado de los Recursos Tecnológicos

Tabla de contenido

1 Objetivo

Garantizar la protección de la disponibilidad, integridad y confidencialidad de la información del Ministerio de Educación, a través del buen uso de los recursos (correo electrónico, internet, redes sociales, hardware, equipo de cómputo, uso de software legal y derechos de autor, acceso inalámbrico) que le son asignados a los colaboradores y terceros para el cumplimiento de sus funciones.

2 Alcance

Lo definido en la presente guía aplica para todos los colaboradores y terceros del MEN.

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).

- **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.
- **Software base:** Cada equipo de cómputo está configurado con el Hardware y Software básico necesario para su funcionamiento: Sistema operativo: Windows, IOS o Linux, Ofimática: Office 365 (Acces, Excel, OneNote, One Drive, Outlook, Power Point, Publisher, Word.), CA, ISE, Software para descomprimir Archivos: Winrar, Antivirus, Chat y conferencias: Teams y Video Conferencias: Webex y teams.

4 Directrices

4.1 Uso de correo electrónico

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar que los colaboradores tomen conciencia de sus responsabilidades sobre el uso adecuado de los recursos que se les asignan para el cumplimiento de sus funciones y así se preservar la seguridad de la información.	Utilizar el correo electrónico exclusivamente para las actividades propias del desempeño de las funciones o actividades laborales en el Ministerio y no se debe utilizar para otros fines.	Todos los colaboradores y terceros del MEN	N.A.
	Abstenerse de recibir y/o contestar PQRSD por medio del correo electrónico, ya que este no es un canal oficial para tal fin. De ser así este tipo de comunicaciones debe trasladarla al área encargada para ser registrada en el sistema de atención al ciudadano.		N. A
	Utilizar el correo electrónico de manera ética, razonable, eficiente, responsable, no abusiva y sin generar riesgos para la operación de equipos o sistemas de información ni para la imagen de MEN.		N.A.
	Responder por todas las actividades que se ejecuten con sus credenciales de acceso a los buzones de correo.		N.A.
	Dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos. Así mismo, evitar prácticas o usos que puedan comprometer la seguridad de la información del MEN.		N.A.
	Respetar el estándar de formato e imagen corporativa definido por MEN en todos los mensajes enviados y conservar, en todos los casos, el mensaje legal corporativo.		N.A.
	Etiquetar los mensajes de correo electrónico de acuerdo con los niveles de clasificación para los cuales se requiere etiquetado (Reservado o Confidencial), de acuerdo con la clasificación y etiquetado de la información establecida en el MEN.		N.A.
	Reportar cuando reciba correos de tipo SPAM, es decir correo no deseado o no solicitado, correos de dudosa procedencia o con virus a la mesa de ayuda de tecnología, con el fin de tomar las acciones necesarias que impidan el ingreso de ese tipo de correos. De la misma forma, el usuario debe reportar cuando no reciba correos y este seguro que este no es de tipo SPAM, así la mesa de ayuda de tecnología hace el análisis para evaluar el origen y así tomar las medidas pertinentes.		N.A.
	Abstenerse de enviar correos masivos que no hayan sido previamente autorizados a través del procedimiento formal de solicitud de cuentas de usuario, establecido en MEN.		N.A.
	Abstenerse de enviar correos que promuevan la discriminación basada en raza, nacionalidad, género, edad, estado marital, orientación sexual, religión o discapacidad, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluidas el lavado de		N.A.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	activos, que contengan amenazas o mensajes violentos.		
	Asegurar que todo mensaje electrónico dirigido a otros dominios debe contener una sentencia o cláusula de confidencialidad.		N.A.
	Asegurar que, en el reenvío de correos electrónicos, la dirección de destino es correcta, de manera que esté siendo enviado a los destinatarios que son.		
	Realizar la depuración periódica del buzón para evitar que alcance su límite.		N.A.
	Reportar los mensajes cuyo origen sea desconocido, y asumir la responsabilidad de las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto.		N.A.
	Abstenerse de suscribirse en boletines en líneas, publicidad o cualquier suscripción que no tenga que ver con sus actividades laborales, con el correo institucional.		N.A.
	Abstenerse de responder mensajes donde les solicitan información personal o financiera que indican que son sorteos, ofertas laborales, ofertas comerciales o peticiones de ayuda humanitaria. Por el contrario, debe notificar este hecho a la OTSI, con el fin de ejecutar las actividades pertinentes como bloquear por remitente y evitar que esos mensajes lleguen a más buzones de correo del MEN.		N.A.
	Abstenerse de enviar, reenviar o intercambiar correos no deseados o considerados como SPAM, cadena del mensajes o publicidad o con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.		N.A.
	Abstenerse de crear, almacenar o intercambiar mensajes que atenten contra las leyes de derechos de autor, divulgar información no autorizada propiedad del MEN, enviar, crear, modificar o eliminar mensajes de otro usuario sin su autorización, abrir o hacer uso y revisión no autorizada de la cuenta de correo electrónico de otro usuario sin su autorización, adulterar o intentar adulterar mensajes de correo electrónico.		N.A.
	Seguir los procedimientos y planes de comunicación interna y externa.		N.A.
	Aprobar y firmar, un documento de análisis de riesgos para la autorización de sistemas de correo electrónico.	Director, Jefe de Oficina, Subdirector, Coordinador de Grupo de Trabajo o Supervisor de contrato	Mesas de ayuda de Tecnología
	Autorizar la asignación de correo electrónico institucional a los colaboradores o terceros que cuenten con un vinculo directo o contrato con el Ministerio.		Mesas de ayuda de Tecnología

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Asignar y controlar el servicio de correo electrónico autorizado por el MEN, el cual cumple con todos los requerimientos técnicos y de seguridad necesarios para evitar ataques informáticos, virus, spyware y otro tipo de software o código malicioso.	Oficina de Tecnología y Sistemas de Información	Reportes de la herramienta Oficce 365
	Revisar junto con cualquier instancia de vigilancia y control todas las comunicaciones establecidas mediante el correo electrónico en caso de una investigación o incidentes de seguridad de la información, ya que sus buzones y copias de seguridad se consideran de propiedad del MEN.		Consola de la herramienta Oficce 365
	Realizar la copia de respaldo de la información (Back up) de manera periódica y segura sobre el servicio de correo electrónico.		Consola de la herramienta Oficce 365
	Asignar el tamaño del buzón de correo electrónico y administrar su capacidad.		Consola de la herramienta Oficce 365
	Realizar copia de respaldo de Información de los registros de auditoría que generan los buzones de correo.		Registros de socialización y apropiación de la política.
	Desbloquear las cuentas creadas en los dominios del MEN a través de la mesa de ayuda, ya que serán bloqueadas automáticamente después de estar inactivas por un tiempo de noventa (90) días.		Consola de la herramienta Oficce 365
	Filtrar los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán revisados para evitar que tengan virus u otro programa destructivo. Si el virus u otro programa destructivo no pueden ser eliminados, el mensaje será borrado.		Consola de la herramienta Oficce 365
	Hacer seguimiento si una cuenta de correo es interceptada por personas mal intencionadas o delincuentes informáticos (crackers) o se reciba cantidad excesiva de correos no deseado (SPAM), para identificar lo sucedido y que se tomen las acciones.		Consola de la herramienta Oficce 365

4.2 Uso de internet

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades sobre el uso adecuado de los recursos que se les asignan para el cumplimiento de sus funciones y así se preservar la seguridad de la información.	Dar cumplimiento a la reglamentación y leyes, en especial la Ley 1273 de 2009 de Delitos Informáticos. Así mismo, evitar prácticas o usos que puedan comprometer la seguridad de la información del MEN.	Todos los colaboradores y terceros del MEN	N.A.
	Informar si tienen accesos a contenidos o servicios que no estén autorizados y no correspondan a sus funciones o actividades designadas dentro del MEN, para que de esta forma la OTSI realice el ajuste de permisos requerido.		N.A.
	Utilizar el acceso a internet única y exclusivamente para el desempeño de las funciones y actividades desarrolladas durante su permanencia en el MEN; Por ninguna razón puede hacer uso para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad y privacidad de la información, la seguridad de la información, del MEN.		N.A.
	Evitar prácticas o usos que puedan comprometer los recursos tecnológicos o que afecte la seguridad y privacidad de la información del MEN.		N.A.
	Abstenerse de asumir en nombre del MEN, posiciones personales en encuestas de opinión, foros u otros medios similares.		N.A.
	Revisar y/o monitorear todas las comunicaciones establecidas mediante el servicio de internet o cualquier instancia de vigilancia y control en caso de ser necesario.	Oficina de tecnología y sistemas de información	Logs dispositivos de seguridad
	Instalar y configurar el navegador autorizado para el uso de Internet en la red del MEN, el cual debe cumplir con todos los requerimientos técnicos y de seguridad necesarios para prevenir ataques de virus, spyware y otro tipo de software o código malicioso.		Plantilla de instalación
	Controlar la conexión de módems externos o internos en la red del MEN, para acceder a internet.		Logs dispositivos de seguridad
	Realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los usuarios. Así mismo, revisar, registrar y evaluar las actividades realizadas durante la navegación.		Logs dispositivos de seguridad

4.3 Uso de redes sociales

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades sobre el uso adecuado de los recursos que se les asignan para el cumplimiento de sus funciones y así se preservar la seguridad de la información.	Abstenerse de asumir en nombre del MEN, posiciones personales en encuestas de opinión, foros u otros medios similares.	Todos los colaboradores y terceros del MEN	N.A.
	Evitar prácticas o usos inapropiados de las redes sociales que puedan comprometer la seguridad y privacidad de la información del MEN.		N.A.
	Hacer buen uso de forma correcta y moderada de las redes sociales, teniendo en cuenta que constituyen un complemento de varias actividades que se realizan por estos medios y para el desempeño de las funciones y actividades a desempeñar en el MEN.		N.A.
	Evitar prácticas o usos que puedan comprometer la seguridad y privacidad de la información del MEN por parte de colaboradores autorizados para hacer uso de los servicios de Redes Sociales.		N.A.
	Utilizar el servicio de redes sociales por los colaboradores y terceros autorizados exclusivamente para el desarrollo de las actividades relacionadas con el MEN.		N.A.
	Hacer buen uso, de forma correcta y moderada de las herramientas complementarias a las redes sociales por parte de los colaboradores autorizados.		N.A.
	No descargar programas ejecutables o archivos que puedan contener software o código malicioso.		N.A.
	No se permite difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.		N.A.
	No se permiten descargas, distribución de material obsceno y no autorizado, degradante, terrorista, abusivo o calumniante a través del servicio de Redes Sociales.		N.A.
	No se permite intentar acceder de forma no autorizada a los sistemas de seguridad del servicio de internet del MEN, o aprovechar el acceso a Redes Sociales para fines ilegales.		N.A.
	Administrar y controlar los accesos a las redes sociales sobre los usuarios autorizados.	Oficina de Tecnología y Sistemas de Información	Logs dispositivos de seguridad

4.4 Uso de Recursos Tecnológicos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar que los empleados y contratistas	Evitar prácticas o usos que puedan comprometer los recursos tecnológicos o que afecte la seguridad y privacidad de la información del MEN.	Todos los colaboradores y Terceros del MEN	N.A.
	No descargar programas ejecutables o archivos que puedan contener software o código malicioso.		N.A.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	No difundir cualquier tipo de virus o software de propósito destructivo o malintencionado.		N.A.
	Hacer buen uso de los recursos tecnológicos del MEN. En ningún momento pueden ser usados para beneficio propio o para realizar prácticas ilícitas o mal intencionadas que atenten contra otros, colaboradores y terceros, legislación vigente o políticas ni lineamientos de seguridad de la información establecidas por MEN.		N.A.
	Efectuar el respaldo de la información que maneja en su equipo de cómputo mediante la herramienta suminstrada por la OTSI (Onedrive)		N.A.
	Entregar todo activo de propiedad del Ministerio, asignado a un colaborador y tercero del MEN, al finalizar el vínculo laboral o contractual o por cambio de cargo si es necesario. Esto incluye los documentos corporativos, equipos de cómputo (Hardware y Software), dispositivos móviles, tarjetas de acceso, manuales, tarjetas de identificación y la información que tenga almacenada en dispositivos móviles o removibles.		N.A.
	No crear y compartir carpetas dentro de sus equipos de computo.		N.A.
	Utilizar únicamente software legalmente adquirido y/o autorizado por el MEN.		N.A.
	No alterar la configuración de los dispositivos asignados, incluyendo sus periféricos.		N.A.
	No abrir los equipos de cómputo, ni tampoco sacar o cambiar componentes de estos.		N.A.
	Reportar de inmediato a la mesa de ayuda de tecnología en caso de que un equipo de cómputo presente un mal funcionamiento.		N.A.
	Instalar el software base en los equipos de cómputo del MEN.	Oficina de Tecnología y Sistemas de Información	Solicitudes de mesa de ayuda de tecnología.
	Evaluar para su aprobación o denegación cualquier requerimiento que tenga un usuario respecto a instalación, desinstalación o actualización de sus aplicaciones, el cual deberá tramitarse por medio de la mesa de ayuda de tecnología.		Solicitudes de mesa de ayuda de tecnología.
	Definir la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas en el MEN para ser instaladas en las estaciones de trabajo de los usuarios.		Inventario de mesa de servicios de CA.
	Realizar el control y verificación del cumplimiento del licenciamiento del software y aplicaciones instaladas en los equipos.		Inventario de mesa de servicios de CA.
	Realizar cambios relacionados con la configuración de los equipos, como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.		Políticas dentro del Directorio Activo
	Administrar de forma remota los dispositivos, equipos o servidores de la infraestructura de procesamiento de información del Ministerio		Políticas dentro del Directorio Activo

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Asignar los recursos tecnológicos (correo electrónico, internet, sistemas de información, equipode computo, impresora, etc) solo a los colaboradores o terceros que cuenten con un vinculo directo o contrato con el Ministerio.		Solicitudes de mesa de ayuda de tecnología.
	Desinstalar software no autorizado de los equipos de los colaboradores sin que sea necesaria su autorización		Solicitudes de mesa de ayuda de tecnología.
	Deshabilitar o inactivar los usuario en los sistemas de información después de cuarenta y cinco (45) días de inactiviad		Inventario de usuario del sistema de información
	Borrado de los usuarios e información de estos después de cuarenta y cinco (45) días después de haberlos deshabilidato o inactivado.		Inventario de usuario del sistema de información

4.5 Uso del software legal y derechos de Autor

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades sobre el uso adecuado de los recursos que se les asignan para el cumplimiento de sus funciones y así se preservar la seguridad de la información	Utilizar software legalmente adquirido o autorizado por el MEN.	Todos los colaboradores y Terceros del MEN	N.A.
	En caso de presentarse algún tipo de reclamación por software ilegal, esta recaerá sobre el usuario responsable del equipo en donde se encontrase instalado dicho software debido a que está atentando contra los derechos de autor.		N.A.
	En presentaciones, documentos, informes y demás documentos que utilicen los usuarios para funciones de su cargo, debe mencionarse la fuente de donde se extrajo la información.		N.A.
	No realizar copias de software que se encuentre instalado o sea desarrollado por el MEN, para su distribución ni para su uso personal.		N.A.
	Instalar y recomendar a las áreas software que cumpla con las leyes de derechos de autor	Oficina de Tecnología y Sistemas de Información	Solicitudes de Mesa de ayuda de tecnología
	Solicitar a la Oficina de Tecnologia y Sistemas de Información, recomendaciones para la adquisición, instalación o uso de software dentro de la entidad.	Procesos del MEN	Solicitudes de Mesa de ayuda de tecnología

4.6 Acceso Inalámbrico

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar que los empleados y contratistas tomen conciencia de sus responsabilidades sobre el uso adecuado de los recursos que se les asignan para el cumplimiento de sus funciones y así se preservar la seguridad de la información.	El uso de la red inalámbrica será exclusivo para usuarios de planta y contratistas con vínculo directo con el MEN, se habilitará el servicio previa solicitud, justificación y autorización a la mesa de servicios de tecnología. Para accesos a dispositivos móviles, se realizará solo previa solicitud y justificación a la mesa de servicios de tecnología.	Todos los colaboradores y Terceros del MEN	N.A.
	Si alguna persona externa al MEN necesita acceso a la red inalámbrica del MEN, deberá solicitarlo accediendo a la red “INVITADO” suministrando los datos allí solicitados y enviar la solicitud al usuario del MEN para aprobación.		N. A
	La información que se maneja dentro del MEN, es propiedad de este y no puede ser divulgada, a no ser que esté autorizado su divulgación.		N.A.
	Crear, administrar todas las redes wifi que sean necesarias para la operacion	Oficina de Tecnología y Sistemas de Información	Solicitudes de Mesa de ayuda de tecnología
	Conceder o denegar accesos a las redes wifi que lleguen a la mesa de ayuda de tecnología.		Solicitudes de Mesa de ayuda de tecnología

4.7 Información de contacto

Cualquier inquietud relacionada con política de uso adecuado de los recursos, favor remitirla al correo seguridaddigital@mineducacion.edu.co.

4.8 Revisión de la guía

Esta guía debe ser revisada por la OTSI como mínimo una vez al año.

4.8.1 Referentes

4.8.1.1 Referentes Normativos

- Norma ISO 27001
- Dominio A.8 Gestión de Activos
- Numeral 8.1.3 Uso aceptable de los activos - Políticas de Seguridad y Privacidad de la Información

4.8.1.2 Referentes de política nacional

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

4.8.1.3 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**	Maura Yuliana Ramírez	**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