Guía - Política de Dispositivos Móviles y Teletrabajo

Tabla de contenido

1 Objetivo

Definir las directrices, responsables y soportes de las políticas de seguridad digital: DISPOSITIVOS MOVILES Y TELETRABAJO, con el fin de preservar la disponibilidad, integridad y confidencialidad de la información del Ministerio de Educación Nacional – MEN.

2 Alcance

Lo definido en la presente guía aplica para los servidores públicos y contratistas del MEN.

3 Definiciones

- **Teletrabajo:** Es una forma de organización laboral, que consiste en el desempeño de actividades remuneradas o prestación de servicios a terceros utilizando como soporte las tecnologías de la información y la comunicación – TIC para el contacto entre el trabajador y la empresa, sin requerirse la presencia física del trabajador en un sitio específico de trabajo.
- **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.
- **Teletrabajador:** Persona que desempeña actividades laborales a través de tecnologías de la información y la comunicación por fuera de la empresa a la que presta sus servicios.
- **Suplementarios:** son aquellos teletrabajadores que laboran dos o tres días a la semana en su casa y el resto del tiempo lo hacen en una oficina**.**
- **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.
- **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
- **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).
- **Dispositivos móviles:** son aquellos dispositivos (portátiles, tabletas y teléfonos móviles) que nos facilitan trabajar fuera de las instalaciones del MEN.
- **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.
- **Escritorio virtual:** es un espacio de trabajo en la nube, donde el servidor público o contratista del MEN encontrará todas las aplicaciones que necesita para trabajar desde cualquier dispositivo o ubicación geográfica.

3.1 Dispositivos móviles

3.1.1 Directrices

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se debe adoptar una política y unas medidas de seguridad de soporte para gestionar los riesgos introducidos por el uso de dispositivos móviles	Llevar un registro y control de todos los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que posee el MEN. (Entrega y recibido de los dispositivos) y hacer firmar por parte del servidores públicos y contratistas el compromiso de cumplimiento de controles.	Subdirección de Gestión Administrativa	Inventario de recursos físicos AD-PR-04 Procedimiento - Administración y control de recursos físicos. Compromiso firmado de cumplimiento de controles para equipos móviles.
	Definir un procedimiento formal de salida de dispositivos de las instalaciones, donde se especifique, entre otras cosas, que el uso de los equipos portátiles de propiedad del MEN, fuera de las instalaciones, únicamente se permitirá a usuarios autorizados mediante una orden de salida, la cual debe tener el visto bueno del jefe inmediato con firma autorizada para este fin.		AD-PR-04 Procedimiento - Administración y control de recursos físicos
	Autorizar la salida de equipos de dispositivos móviles para la ejecución de actividades fuera de las instalaciones del MEN.		Mesa de ayuda de Administrativa
	No permitir la salida de equipos de escritorio para la ejecución de cualquier actividad fuera de las instalaciones del MEN. Cuando por alguna excepción se requiera la salida de un equipo de escritorio deberá tener la autorización previa de la OTSI, con el fin de verificar que tipo de información se encuentra almacenada en este y aplicar controles necesarios antes de su salida.		Mesa de ayuda de Administrativa

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Hacer buen uso de los dispositivos móviles (portátiles, tabletas y teléfonos móviles) que son asignados para el desempeño de sus funciones laborales u obligaciones contractuales.	Servidores públicos y contratistas del MEN	Compromiso firmado de cumplimiento de controles para equipos móviles.
	Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para todos los dispositivos móviles, como celulares, que almacenen información del MEN.		N/A
	Utilizar en los dispositivos móviles únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.		N/A
	Mantener apagado el bluetooth o cualquier otra tecnología inalámbrica que exista o llegara a existir.		N/A
	Utilizar los equipos móviles asignados por el MEN exclusivamente para desempeñar las funciones asignadas al cargo o las obligaciones contractuales pactadas.		N/A
	El uso de los escritorios móviles asignados debe ser exclusivo del servidor público o contratista, por lo tanto, no debe realizar préstamos de estos.		N/A
	No instalar ni configurar en los servicios ni en la infraestructura tecnológica del MEN (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: • Gotomypc, • Teamviewer, • LogMeIn, • AnyDesk, • Etc.		N/A
	Implementación de los controles apropiados para proteger los dispositivos móviles, que son autorizados para salir de las instalaciones, como son: identificación de tipo de dispositivo, versión de aplicaciones instaladas, restricción en la ejecución de aplicaciones de acuerdo con las que están permitidas, contenido restringido, de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, y de ser necesario, se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos entre otros.	Oficina de Tecnología y Sistemas de Información	Configuración de cada equipo, en los dispositivos de seguridad de la OTSI.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Asegurar que los dispositivos móviles provistos por el MEN cuenten con los siguientes controles: 1. Uso de usuario y contraseña para acceso al mismo. 2. Uso de software antivirus provisto por el MEN. 3. Restricción de privilegios administrativos para los usuarios. 4. Uso de software licenciado y provisto por el MEN (Software base) 5. Realización de copias de seguridad periódicas. 6. Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos como OneDrive y cifrado de la información. 7. Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.		
	Derecho a revisar la utilización del dispositivo móvil ante cualquier indicio de un uso inapropiado del mismo, inspeccionarlo o disponer de el de cualquier forma, dado que tanto el dispositivo móvil como la información almacenada es propiedad del MEN.		N/A

3.2 Teletrabajo

3.2.1 Directrices

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Hacer buen uso de los dispositivos de los escritorios virtuales que son asignados para el desempeño de sus funciones laborales u obligaciones contractuales.	Servidores públicos que apliquen al teletrabajo.	Compromiso firmado de cumplimiento de controles de seguridad de la información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Contar con un sistema de autenticación, como un patrón, código de desbloqueo o una clave, para el equipo de cómputo donde se utilizará el escritorio virtual, que almacenen información del MEN.		N/A
	Realizar periódicamente copias de respaldo de la información. Para la información almacenada en los escritorios virtuales que son entregados por el MEN debe estar almacenada en OneDrive.		OneDrive.
	Utilizar en los escritorios virtuales únicamente redes seguras y con la protección adecuada para evitar acceso o divulgación no autorizada de la información almacenada y procesada en ellos.		N/A
	Acatar el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.		N/A
	El uso de los escritorios móviles asignados debe ser exclusivo del servidor público, por lo tanto, no debe realizar préstamos de estos.		N/A
	No instalar ni configurar en los servicios ni en la infraestructura tecnológica del MEN (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: • Gotomypc, • Teamviewer, • LogMeIn, • AnyDesk, • Etc.		N/A
	Implementación de los controles apropiados para proteger los escritorios virtuales, que son autorizados para salir de las instalaciones, como son: identificación de tipo de dispositivo, versión de aplicaciones instaladas, restricción en la ejecución de aplicaciones de acuerdo con las que están permitidas, contenido restringido, de conexión de dispositivos USB, inactivación de accesos inalámbricos cuando se encuentren conectadas a la red LAN, y de ser necesario, se podrá restringir conexiones hacia ciertos servicios de información que sean considerados maliciosos entre otros.	Oficina de Tecnología y Sistemas de Información	Configuración de cada equipo, en los dispositivos de seguridad de la OTSI.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Asegurar que los dispositivos móviles provistos por el MEN cuenten con los siguientes controles: 1. Uso de usuario y contraseña para acceso al mismo. 2. Uso de software antivirus provisto por el MEN. 3. Restricción de privilegios administrativos para los usuarios. 4. Uso de software licenciado y provisto por el MEN (Software base) 5. Realización de copias de seguridad periódicas. 6. Uso de mecanismos de seguridad que protejan la información en caso de pérdida o hurto de los dispositivos como OneDrive y cifrado de la información. 7. Adquisición de pólizas que cubran el hardware y la información de los dispositivos, contra perdida o hurto.		
	Derecho de revisar la utilización de los escritorios virtuales ante cualquier indicio de un uso inapropiado del mismo o inspeccionarlo o disponer de el de cualquier forma, dado que tanto el dispositivo como la información almacenada es propiedad del MEN.		N/A
	Hacer cumplir el procedimiento de Teletrabajo establecido en la normatividad correspondiente vigente tanto externa como interna.	Subdirección de Talento Humano	N/A
	Incluir en el PIC las capacitaciones necesarias sobre las políticas y controles de seguridad de la información para los servidores públicos que apliquen al teletrabajo.		PIC
	Hacer firmar al servidor púbico que aplica al teletrabajo, el compromiso de cumplimiento de controles de seguridad de la información.		Compromiso firmado de cumplimiento de controles de seguridad de la información

3.3 Trabajo remoto

3.3.1 Directrices

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
El MEN debe implementar políticas y medidas de seguridad para la operación de la información a través del trabajo remoto	No instalar ni configurar en los servicios ni en la infraestructura tecnológica del MEN (computadores de escritorio, equipos móviles, servidores de cómputo físicos y virtuales, etc.) software para conexiones remotas gratis o de pago como: • Gotomypc, • Teamviewer, • LogMeIn, • AnyDesk, • Etc.	Servidores públicos y contratistas del MEN	N/A
	Contar con las aprobaciones requeridas para establecer conexión remota (VPN) a los dispositivos de la plataforma tecnológica del MEN y acatar las instrucciones de acceso establecidas para las conexiones remotas.		Manual de acceso a VPN
	Establecer conexiones remotas únicamente a través de las VPN seguras y utilizar computadores en sitios confiables (Ej. Casa) y, en ninguna circunstancia, en computadores públicos, de hoteles o cafés internet, entre otros.		N/A
	Realizar la solicitud de conexiones VPN por medio de la Mesa de Ayuda de Tecnología		Mesa de Ayuda de Tecnologia
	El servidor público o contratista que solicite acceso por medio de una VPN es responsable del uso adecuado del acceso remoto.		N/A
	Evaluar las solicitudes de permisos de VPN, aprobarlas o denegarlas, previa autorización por el responsable de la Dependencia de la cual depende el servidor público o contratista que solicita el permiso.	Oficina de Tecnología y Sistemas de Información	Mesa de ayuda de tecnología ST-FT-05 Formato Solicitud de Conexión VPN ST-FT-06 Formato Solicitud de Conexión VPN CLIENT TO SITE Respuesta a solicitud VPN asignada
	Configurar las conexiones remotas a los servicios tecnológicos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores asignadas dentro del MEN.		

3.3.2 Información de contacto

Cualquier inquietud relacionada con política para dispositivos móviles, teletrabajo y trabajo remoto favor remitirla al correo seguridaddigital@mineducacion.gov.co.

3.3.3 Revisión de la guía

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

3.3.4 Referentes

3.3.4.1 Referentes Normativos

- Norma ISO 27001
- Dominio A.6.2 Dispositivos móviles y teletrabajo – Control A.6.2.1 Política para dispositivos móviles
- Dominio A.6.2 Dispositivos móviles y teletrabajo – Control A.6.2.2 Teletrabajo

3.3.4.2 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 -

3.3.4.2.1 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	**Cargo**	Profesional Especializado -	**Cargo**	Jefe de la Oficina de Tecnología y Sistemas de

	Oficina de Tecnología y Sistemas de Información		Subdirección de Desarrollo Organizacional.		Información