Guía - Política Control de Acceso

Tabla de contenido

1 Objetivo

Definir las directrices generales para limitar el acceso a la información, instalaciones de procesamiento de información y a los servicios de tecnología (Red, servicios asociados, sistemas de información) a los colaboradores y terceros del MEN.

2 Alcance

Lo definido en la presente guía aplica para todos los colaboradores y terceros que cuenten con accesos a la información, los servicios de tecnología (Red, servicios asociados, sistemas de información) 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).
- **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 Control de Acceso

4.1.1 Directrices

4.1.1.1 Control de acceso

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	Definir los roles y perfiles de los usuarios con acceso a los activos de información de cada proceso, teniendo en cuenta los riesgos de seguridad de la información asociados a cada uno de ellos.	Líderes de procesos	Directorio Activo
	Controlar el uso de la información para prevenir los accesos no autorizados. Los privilegios sobre la información deben ser otorgados y mantenidos de acuerdo con las necesidades de la operación, limitando el acceso sólo a lo que es requerido.	Oficina de tecnología y sistemas de información	Directorio Activo
	Diseñar, documentar e implementar los controles necesarios para el acceso la infraestructura tecnológica (Redes, Correo, Internet, Sistemas de información, Información etc.) y así preservar la confidencialidad, integridad y disponibilidad de la información).		Documentos SGSI

4.1.1.2 Acceso a redes y a servicios de red

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente	Dar el acceso a la red de la Entidad solo a usuarios autorizados, previa definición, verificación y control de los perfiles y roles para el acceso en los diferentes sistemas de información, en coordinación con Subdirección de Talento Humano y la Subdirección de Contratación	Oficina de Tecnología y Sistemas de Información	Mesa de ayuda de Tecnologia.
	Proveer una red a invitados para el acceso a internet y consulta a los sistemas de información públicos de la entidad.		Consola de administración ISE
	Definir los roles y perfiles de usuarios de redes mediante la solución ISE.		Consola de administración ISE
	Autorizar la conexión a nivel remoto de los colaboradores o terceros que por su labor lo requieran La conexión remota a la red de área local del Ministerio debe ser establecida a través de una conexión VPN segura aprovisionada por el MEN y velar porque cuente con el monitoreo y registro de las actividades necesarias.		Mesa de ayuda de Tecnologia.

	Efectuar el seguimiento a los accesos realizados por los usuarios mediante el registro de eventos en los diversos componentes de la plataforma tecnológica, con el fin de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información		Logs de eventos

4.1.1.3 Administración de accesos.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	Almacenar las contraseñas de usuarios administradores utilizando cifrado de una sola vía en un sistema informático protegido mediante tecnologías diferentes a las utilizadas para la identificación y autenticación de usuarios.	Oficina de Tecnología y sistemas de Información	Informe Operador de servicios TI.
	Definir los parámetros para que los sistemas de administración de contraseñas para usuarios de correo, bases de datos, sistemas de información y redes del MEN cumplan como mínimo con las siguientes especificaciones: ○ Obligar el uso de usuarios y contraseñas individuales para determinar responsabilidades en los accesos a los activos de información. ○ Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de estas o cuando consideren que la misma ha sido comprometida, e incluir un procedimiento de confirmación para contemplar los errores de ingreso. ○ Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información. ○ No permitir mostrar las contraseñas en texto claro cuando son ingresadas. ○ Verificar que la longitud de la contraseña sea de al menos doce (12) caracteres combinados aleatoriamente entre números, letras minúsculas, letras mayúsculas y símbolos.		Portal de identidades
	Responder por el uso de sus credenciales de acceso asignadas (usuarios y claves) ya que son de uso personal e intransferible y es responsabilidad del usuario el uso que se haga de las credenciales asignadas.	Todos los colaboradores y tercero del MEN	N.A
	Acceder a los servidores únicamente en las instalaciones del MEN, No debe realizar ninguna actividad de tipo remoto sin la debida autorización.		N.A
	Cambiar sus contraseñas de acceso periódicamente, inclusive antes de que esta expire, de acuerdo con lo establecido por la OTSI.		N.A
	Cambiar las contraseñas suministrada por la mesa de servicio, en su primer inicio de sesión.		N.A

	Dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista.		N.A
	Crear su contraseña en la plataforma (servicios de red, servicios y sistemas de información) que requiera para el desempeño de sus funciones laborales.		

4.1.1.4 Registro y cancelación del registro de usuarios

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios	Solicitar a la OTSI el registro de un usuario nuevo, modificación o cancelación de estos. Los usuarios que no tengan vinculación directa deben tener un dominio diferente a los usuarios de planta y contratista.	Líderes de procesos, directores, jefes de dependencias	Mesa de ayuda de Tecnologia
	Proteger sus contraseñas siguiendo las siguientes recomendaciones: a) Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc. b) Tener mínimo doce caracteres alfanuméricos. c) Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema. d) Cambiarse obligatoriamente cada noventa (45) días, o cuando lo establezca la OTSI. e) Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres (3) anteriores. f) Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario. g) No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos. h) No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse. i) No ser reveladas a ninguna persona, incluyendo al personal la OTSI. j) No registrarlas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.	Todos los colaboradores y tercero del MEN	N.A

	k) No enviar nunca la contraseña por correo electrónico, redes sociales o en un SMS. l) Las contraseñas que se generen en las diferentes aplicaciones deben viajar cifrada por la red. m) No se debe facilitar ni mencionar la contraseña en conversaciones o comunicaciones de cualquier tipo. n) No utilizar en ningún caso contraseñas que se ofrezcan en los ejemplos explicativos de construcción de contraseñas robustas. o) No escribir las contraseñas en equipos de cómputo de los que se desconozca su nivel de seguridad y puedan estar monitorizados, o en ordenadores de uso público (bibliotecas, cibercafés, telecentros, etc.). p) No compartir su contraseña con terceros. El uso de la contraseña es personal e intransferible. q) No revelar su contraseña vía telefónica. r) No utilizar la función "Recordar Contraseña " de programas de aplicación, exploradores de Internet, correo electrónico, o cualquier otro programa. s) Informar cualquier incidente de seguridad que ponga en riesgo su contraseña a la OTSI por medio de la mesa de ayuda de Tecnología. t) Informar a la OTSI por medio de la mesa de ayuda de Tecnología si alguien dentro o fuera del MEN le solicita su contraseña. u) No permita que le observen al escribir su contraseña. v) Cambiar las contraseñas por defecto proporcionadas por desarrolladores/fabricantes. w) Luego de 5 intentos de ingreso de contraseña fallidos, se bloqueará la cuenta de usuario y este deberá solicitar por medio de la mesa de ayuda de Tecnología el desbloqueo de esta. x) Los computadores deben contar con protectores de pantalla protegidos por contraseña que deben ser habilitados dentro de los 5 minutos de inactividad del usuario. y) Los sistemas de información del MEN bloquearan automáticamente las cuentas de los usuarios que no hayan ingresado en los últimos sesenta (60) días. Cuando un usuario inicie sesión por primera vez o cuando se realice una activación del usuario, el sistema exigirá cambio de contraseña. Las contraseñas generadas por primera vez deben estar alineadas a los requisitos y recomendaciones que a continuación se contemplan. Otras recomendaciones para crear las contraseñas:		

	a) No utilizar información personal en la contraseña: nombre del colaborador o de sus familiares, ni sus apellidos, ni su fecha de nacimiento, ni cuentas bancarias, ni tarjetas de crédito, etc. b) Se deben utilizar mínimo 8 caracteres para crear la clave. c) Las contraseñas deben utilizar la combinación aleatoria de los siguientes tipos de caracteres: a. Minúsculas b. Mayúsculas c. Números d. Caracteres especiales como +*! @ # $ & % ^ -/ d) Evitar utilizar secuencias básicas de teclado (por ejemplo:" qwerty", "asdf" o las típicas en numeración: "1234" ó "98765"). e) No repetir los mismos caracteres en la misma contraseña. (ej.: "111222"). f) No se debe utilizar como contraseña, ni contener, el nombre de usuario asociado a la contraseña. g) Las contraseñas no deben ser FECHAS. h) La contraseña no debe basarse en dos palabras separadas por un espacio ( ), guion (-) o guion bajo (_). i) No se deberían asignar contraseñas en blanco. No utilizar datos relacionados con el usuario que sean fácilmente deducibles, o derivados de estos. (ej.: no poner como contraseña apodos, el nombre del actor o de un personaje de ficción preferido, etc.). j) No se deben utilizar palabras que se contengan en diccionarios en ningún idioma. k) Cuando el sistema le solicite cambio de contraseña esta no debe haber sido utilizada en los históricos del sistema. l) Elegir una contraseña que pueda recordarse fácilmente y es deseable que pueda escribirse rápidamente, preferiblemente, sin que sea necesario mirar el teclado. m) Realizar cambio de contraseña como mínimo cada 45 días. n) Las contraseñas deberán tener histórico de 3 claves para que puedan ser repetidas.		
	Establecer los procedimientos para cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información	Oficina de tecnología y sistemas de	Portal de identidades

	Establecer el uso de contraseñas individuales para determinar las responsabilidades de su uso	información	Portal de identidades
	Atender las solicitudes de mesa de ayuda de Tecnología, en donde se realizará la creación, modificación y eliminación de usuarios del directorio activo en el MEN. Sistemas de Administración de Contraseñas.		Mesa de ayuda de Tecnologia
	Definir y aplicar las reglas para que las contraseñas cumplan con los siguientes parámetros: Contener mayúsculas, minúsculas, números, por lo menos un carácter especial y tener una longitud de 12 caracteres.		Portal de identidades
	Definir y aplicar la regla en el sistema para que obligue al usuario a cambiar la contraseña por lo mínimo 1 vez cada 45 días.		Directorio Activo
	Mantener un registro de las 3 últimas contraseñas utilizadas por el usuario, y evitar la reutilización de estas.		Directorio Activo
	Propender porque que las contraseñas se almacenen de forma cifrada utilizando un algoritmo de cifrado unidireccional.		Directorio Activo / Portal de identidades

4.2.2 Suministro de acceso de usuarios

4.2.2.1 Gestión de altas/bajas en el registro de usuarios y contraseñas de usuarios de correo, bases de datos, sistemas de información y redes.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de	Solicitar la asignación, modificación o revocación de privilegios en los Sistemas de Información del MEN.	Líderes de procesos, directores, Jefes de dependencias	
	Notificar a la OTSI mediante correo electrónico o por medio de la mesa de ayuda de tecnología, la creación, modificación o bloqueo de la cuenta de usuario; esta solicitud se analizará por parte de la OTSI con el fin de su autorización. En caso de requerirse modificaciones y/o aclaraciones, se enviará un correo al área requirente solicitándolas.	Todos los colaboradores y tercero del MEN	Correo Electrónico / Mesa de Ayuda de Tecnologia
	Realizar las gestiones asociadas a la creación, modificación o eliminación de contraseñas.	Oficina de tecnología y sistemas de información	Portal de Identidades

4.2.3 Gestión de derechos de acceso privilegiado

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
restringir y controlar la asignación y uso de derechos de acceso privilegiado.	Revisar periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo los derechos de acceso de los usuarios a la Infraestructura Tecnológica, sistemas de información del MEN.	Oficina de tecnología y sistemas de información	Directorio Activo
	Propender porque el uso y creación de contraseñas para usuarios de correos, bases de datos, sistemas de información y redes deben estar alineados con el numeral del buen uso y creación de contraseñas seguras.		Directorio Activo
	Realizar la administración y gestión de los usuarios en todos los sistemas de información y/o aplicaciones del MEN, como área funcional quien, en el conocimiento del negocio, la información, procesos sensibles y niveles de autoridad debe asignar los privilegios teniendo en cuenta las funciones y el rol de cada usuario en el sistema, así como la verificación de identidad cuando el usuario no recuerde los datos de ingreso al sistema y/o este no cuente con mecanismos para dicho proceso.	Jefes de Área Funcional	Logs Sistemas de información

4.2.4 Gestión de información de autenticación secreta de usuarios

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Asignar la información secreta se debería controlar por medio de un proceso de gestión formal.	Pedir a los usuarios que firmen una declaración para mantener confidencial la información de autenticación secreta personal, y mantener la información de autenticación secreta del grupo (es decir, compartida) únicamente dentro de los miembros del grupo; esta declaración firmada se puede incluir en los términos y condiciones del empleo.	Oficina de tecnología y sistemas de información	Contrato
	Modificar la información de autenticación secreta por defecto, del fabricante, después de la instalación de los sistemas o software.		Guías de Hardening

4.2.5 Revisión de los derechos de acceso de usuarios

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
revisar los derechos de acceso de los usuarios, a intervalos	Revisar los derechos de acceso de los usuarios a intervalos regulares y después de cualquier cambio, promoción, cambio a un cargo a un nivel inferior, o terminación del empleo. Al menos, cada año, se realizará una revisión de los privilegios de acceso de todos los usuarios.	Líderes de procesos, directores, Jefes de dependencias	Portal de identidades

Cuando se trate de privilegios especiales (administrador, root, etc.), tal revisión de privilegios se deberá realizar, al menos, 2 veces al año, y, en cualquier caso, siempre que existan: a) Alta de nuevos usuarios. b) Baja de usuarios. c) Además, los privilegios de acceso de usuarios, tanto internos como externos, deben ser revisados siempre que existan cambios en las funciones o responsabilidades. Para ambos tipos de usuarios se tendrán en cuenta, al menos, las siguientes cuestiones: 1. Necesidad de nuevos permisos. 2. Cancelación de antiguos permisos. 3. Segregación de funciones. 4. Devolución de activos y modificación o cancelación de permisos de accesos físicos. 5. Modificación de contraseñas de acceso. 6. Notificación al personal implicado de su baja o cambio. 7. Necesidad de retención de registros.		
Revisar las autorizaciones para los derechos de acceso privilegiado a intervalos más frecuentes.		Portal de identidades
Verificar a intervalos regulares las asignaciones de privilegios para asegurar que no se hayan obtenido privilegios no autorizados.		Portal de identidades
Comunicar a la Subdirección de Talento Humano y Subdirección de Contratación, el cambio de cargo, funciones o actividades o la terminación contractual de los Colaboradores pertenecientes al proceso.		Correo electrónico /Mesa de ayuda de administrativa y talento humano
Realizar labores periódicas de monitorización de los sistemas con el fin de detectar accesos no autorizados y desviaciones, registrando eventos que suministren evidencias en caso de producirse incidentes relativos a la seguridad.	Oficina de Tecnología y sistemas de Información	

	Revisar conjuntamente con la OTSI los derechos de acceso de los usuarios a la información y a la plataforma tecnológica y de procesamiento de información del MEN, periódicamente y cada vez que se realicen cambios de personal en los procesos o grupos de trabajo.		
	Realizar las revisiones periódicas para la verificación del cumplimiento de los lineamientos, se tendrán en cuenta los registros de eventos y de uso de los sistemas descritos a continuación: Registro de eventos: La OTSI contempla que el sistema de monitoreo debe suministrar como mínimo: a) Intentos de acceso fallidos. b) Bloqueos de cuenta. c) Cuentas inactivas y deshabilitadas. d) Últimos accesos a cuentas. entre otros. Registro de uso de los sistemas: a) Accesos no autorizados. b) Uso de privilegios. c) Alertas de sistema. Entre otros		Portal de identidades

4.2.6 Retiro o ajuste de los derechos de acceso

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Retirar los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de	Comunicar a la Subdirección de Talento Humano y Subdirección de Contratación, el cambio de cargo, funciones o actividades o la terminación contractual de los colaboradores pertenecientes al proceso.	Todas las dependencias del MEN	Correo electrónico /Mesa de ayuda de administrativa y talento humano
	Comunicar a la OTSI sobre estas novedades, con el fin de retirar los derechos de acceso a los servicios informáticos y de procesamiento de información	Subdirección de Talento Humano y Subdirección de Contratación	Correo electrónico /Mesa de ayuda de Tecnologia
	Retirar todos los privilegios de accesos de usuarios de correo, bases de datos, sistemas de Información y redes tanto internos como externos en el momento de la finalización de su contrato o prestación de sus servicios en el MEN.	Oficina de Tecnología y	Directorio Activo

	Remover los accesos lógicos a los activos de información por los administradores de sistemas de forma inmediata.	Sistemas de Información	Logs de sistemas d información
	Inactivar las cuentas de acceso de correo, bases de datos, sistemas de Información y redes.		Directorio Activo

4.3 Responsabilidades de los usuarios

4.3.1 Uso de información de autenticación secreta

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación	Mantener la confidencialidad de la información de autenticación secreta, asegurándose de que no sea divulgada a ninguna otra parte, incluidas las personas con autoridad.	Todos los colaboradores y terceros del MEN	Logs sistemas de información
	Evitar llevar un registro (por ejemplo, en papel, en un archivo de software o en un dispositivo portátil) de autenticación secreta, a menos que se pueda almacenar en forma segura y que el método de almacenamiento haya sido aprobado (por ejemplo, una bóveda para contraseñas).		
	Cambiar la información de autenticación secreta siempre que haya cualquier indicio de que se pueda comprometer la información.		Directorio Activo
	✓ Cambiar las contraseñas suministrada por la mesa de servicios en su primer inicio de sesión ✓ Dar buen uso a las claves de acceso suministradas y no deben escribirlas o dejarlas a la vista. ✓ No prestar, divulgar o difundir la contraseña de acceso asignadas a compañeros, jefes u otras personas que lo soliciten. ✓ Dar cumplimiento a las políticas de seguridad de la información de uso y selección de las contraseñas de acceso, por lo tanto, son responsables de cualquier acción que se realice utilizando el usuario y contraseña asignados. ✓ Evitar revelar las contraseñas por vía telefónica, correo electrónico o por ningún otro medio. ✓ Reportar a la OTSI sobre cualquier incidente o sospecha de que otra persona esté utilizando su contraseña o usuario asignado. ✓ Reportar a la OTSI sobre cualquier sospecha o evidencia de que una persona esté utilizando una contraseña y usuario que no le pertenece.		

	✓ Activar protectores de pantalla con contraseñas, si debe abandonar la estación de trabajo momentáneamente, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada. ✓ Dar buen uso del acceso al correo, Bases de Datos, Sistemas de Información y Redes y responder por las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos. ✓ Utilizar responsablemente y no compartir sus cuentas de usuario y contraseñas con otros colaboradores o con personal provisto por terceras partes. ✓ Cumplir con las políticas del MEN definidas en el presente Manual, también aplica para los colaboradores que les fuese asignada una cuenta y contraseña de otras entidades. ✓ Cumplir los lineamientos y políticas para la configuración de cuentas de usuario y contraseñas implantados por el MEN, con el fin de asegurar una gestión y administración adecuada de las cuentas de usuario y contraseñas. ✓ Realizar sus propios respaldos en la aplicación de respaldo en la nube entregada por el MEN (OneDrive). ✓ Usar de forma adecuada los recursos de red y de seguir los procedimientos definidos para el acceso a las redes. ✓ Acceder a los recursos de servicios de información a través de la cuenta de usuario asignada. Proteger sus contraseñas y seguir las recomendaciones de uso y creación de contraseñas seguras.		
	Asegurar la protección apropiada de contraseñas cuando se usan éstas como información de autenticación secreta en procedimientos de ingreso automatizados, y estén almacenadas.		
	No usar la misma información de autenticación secreta para propósitos de negocio y otros diferentes de estos.		

4.4 Control de acceso a sistemas y aplicaciones

4.4.1 Restricción de acceso a la información

4.4.1.1 Control de identificación y autenticación de usuarios de correo, bases de datos, sistemas de información y redes.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

restringir de acuerdo con la política de control de acceso.	Define que todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.	Oficina de tecnología y sistemas de información	
	Restringir el acceso a terceros a los servicios, infraestructura y sistemas no autorizaros por la entidad. De ser necesario el acceso de estos se realizará por medio del Operador de servicios TI.		Mesa de ayuda de Tecnologia

4.4.1.2 Sesiones Inactivas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
restringir de acuerdo con la política de control de acceso.	Activar protectores de pantalla con contraseñas, al momento de que el usuario abandone la estación de trabajo momentáneamente, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.	Todos los colaboradores del MEN	
	Asegurar que, los sistemas de información si detectan inactividad por un periodo igual o superior a cinco (5) minutos, deben automáticamente aplicar “timeout”, es decir, finalizar la sesión de usuario.	Oficina de Tecnología y Sistemas de Información	
	Bloquear las cuentas de usuarios del dominio del MEN que no se identifique actividad, ya sea por finalización de su contrato o prestación de sus servicios en el MEN: a) Serán bloqueadas automáticamente después de estar sin actividad en un tiempo de sesenta (60) días. b) Serán inactivadas automáticamente después de estar sin actividad en un tiempo de ciento ochenta (180) días.		

4.4.2 Procedimiento de ingreso seguro

4.4.2.1 Responsabilidades de los colaboradores con respecto al acceso a: correo, bases de datos, sistemas de información y redes.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Evitar el acceso no autorizado a sistemas y aplicaciones	Responder por las acciones realizadas en el correo, bases de datos, sistemas de información y redes, así como del uso del usuario y contraseña asignados para el acceso a estos.	Todos los colaboradores y terceros del MEN	
	No deben compartir sus cuentas de usuario y contraseñas con otros colaboradores ni con personal provisto por terceras partes.		
	A los colaboradores que les fuese asignada una cuenta y contraseña de otras entidades deberán cumplir tanto con las políticas del MEN como las políticas de seguridad del MEN que asigna dicha cuenta.		
	Acogerse los lineamientos y políticas para la configuración de cuentas de usuario y contraseñas implantados por el MEN todos los colaboradores y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información del MEN con el fin de asegurar una gestión y administración adecuada de las cuentas de usuario y contraseñas.		
	Definir y ejecutar los lineamientos para las cuentas, creadas en los dominios del MEN, asignadas a las secretarias a las cuales el MEN presta servicios: a) Serán bloqueadas automáticamente después de estar sin actividad en un tiempo de sesenta (60) días. b) Serán inactivadas automáticamente después de estar sin actividad en un tiempo de ciento ochenta (180) días. c) Serán administradas por la OTSI.	Oficina de Tecnología y Sistemas de Información	

4.4.2.2 Acceso a las bases de datos y sistemas de información.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Operar toda la información del MEN únicamente a través de un mismo tipo de sistema manejador de base de datos y de los sistemas de información del MEN para beneficiarse de los mecanismos de integridad, seguridad y recuperación de información en caso de presentarse alguna falla.	Oficina de tecnología y sistemas de información	
	Definir los privilegios o niveles de seguridad de acceso mínimos requeridos para el acceso del operador de servicios TIC a los sistemas de información, con el fin de buscar la seguridad total de la información del MEN. Los niveles de seguridad de acceso deberán controlarse por un administrador único y poder ser gestionados por software.		Directorio Activo

	Respaldar los datos de los sistemas de información de acuerdo con la frecuencia de actualización de sus datos, guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados.		
	Definir un proceso que permita verificar que las copias de respaldo se hayan realizado exitosamente.		
	Asegurar que los sistemas de información contemplen el registro histórico de las transacciones sobre datos relevantes, así como el usuario y fecha en que se realizó (Normas Básicas de Auditoría y Control).		
	Implantar rutinas periódicas de auditoría a la integridad de los datos, de las copias de seguridad y de los programas de cómputo, para asegurar su confiabilidad.		
	Asegurar que todos los sistemas de información que se tengan en operación deben contar con el protocolo de paso a producción cuando haya versiones nuevas por corrección de errores, nuevas funcionalidades o la incorporación de nuevas tecnologías.		ST-PT-01 Protocolo de Paso a Producción para la Entrega en Productivo de Nuevas Soluciones Tecnológicas
	Realizar sus propios respaldos en la aplicación de respaldo en la nube entregada por el MEN (OneDrive) en cuanto a la información de los equipos de cómputo suministrados.	Todos los colaboradores y terceros del MEN	N.A
	Delimitar las responsabilidades en cuanto a quién está autorizado a consultar y/o modificar en cada caso la información, tomando las medidas de seguridad pertinentes.	Líderes de procesos, directores, jefes de dependencias	

4.4.2.3 Autenticación a los sistemas de información usuarios externos.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
restringir de acuerdo con la política de control de acceso.	Activar protectores de pantalla con contraseñas, al momento de que el usuario abandone la estación de trabajo momentáneamente, con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.	Todos los colaboradores del MEN	
	Definir la Estructura de autenticación en el ámbito completo de la aplicación	Oficina de Tecnología y	

	Aplicar los Principios y políticas de la autenticación: a. Toda aplicación que, se conecte a la autenticación centralizada, ya sea Windows, Linux u otro OS debe asegurar que se comunica directamente con el árbol del LDAP. UID (user id): Identificación única de la entrada del árbol. b. Toda aplicación debe ser compatible con los cifrados más fuertes mínimo TLS 1.2 c. Toda aplicación debe cumplir las políticas de seguridad del Ministerio. d. Para el manejo de autenticación negativa o en caso de producirse un error el acceso siempre será negado. e. Si la aplicación tiene que usar cabecera de referencia, deberá únicamente hacerlo con un mecanismo de defensa en profundidad, y no tratar de limpiar su contenido, solo rechazarlo si no es correcto. Todo código tiene errores, así que debe minimizarse la cantidad de código que trata con la cabecera de referencia. f. Toda aplicación debe contar con un mecanismo de protección de autenticación que detecte anomalías, amenazas y posibles ataques de fuerza bruta, diccionario entre otras que son identificadas como posibles ataques. g. Toda aplicación debe tener un registro de logs que permita seguimiento y la elaboración de un informe de acceso a las aplicaciones. h. En el proceso de autenticación, cuando se consultan los datos del usuario que está realizando el intento de acceso, debe comprobarse que sólo se devuelve un registro o ninguno, no permitiendo el acceso si se recupera más de un registro. i. Utilizar siempre métodos POST en los procesos de autenticación. j. Limitar el número de fallos consecutivos permitidos en una autenticación.	Sistemas de Información	

	k. Introducir un retardo que obligue a que pase un tiempo determinado antes de volver a intentar una autenticación se reducen las posibilidades de éxito de los ataques de fuerza bruta. l. No validar la autenticación o autorización en el lado cliente. m. Usar certificados digitales para evitar suplantaciones de identidad de usuarios. n. Asegurar que quien envía el formulario es una persona y no una máquina.		

4.4.2.4 Acceso a las redes

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Preservar la seguridad de los servicios de red garantizando que: a) Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos. b) Se exige control de acceso de los usuarios a los servicios de información. c) Se mantienen instalados y habilitados sólo aquellos servicios y puertos que son utilizados por los sistemas de información y software del MEN. d) Se controla el acceso lógico a los servicios, tanto a su uso como a su administración, mediante bloqueo de puertos en el firewall del MEN. e) El acceso de las redes del MEN es de uso exclusivo y único para la infraestructura provista.	Oficina de tecnología y sistemas de información	

4.4.2.5 Acceso a servidores

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Evitar el acceso no autorizado a sistemas y aplicaciones	Definir que los servidores físicos y virtuales, deben estar bajo un solo administrador (Operador de servicios TICs).	Oficina de tecnología y sistemas de información	
	Los permisos de acceso a los diferentes ambientes están limitados solo al tipo de ambiente requerido; no se debe mezclar los ambientes. Deben ser solicitados por medio de la mesa de ayuda de Tecnología mediante el formato ST-FT-03 Formato Configuración de Políticas de Firewall.		ST-FT-03 Formato Configuración de Políticas de Firewall.

Los servidores físicos y virtuales serán accedidos por consola o por escritorio remoto cumpliendo las reglas definidas a continuación:

Ambiente	Consola y escritorio remoto	Reglas tráfico entrante
Pruebas	Compartido (MEN-Operador de red)	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. b. Permisos de acceso hacia los servidores. 2. Las reglas se depuran cada tres meses. 3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.
Producción	Operador del Servicio	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. 2. Las reglas se depuran cada tres meses.

		3. Evitar reglas provenientes de 'any'. Es preferible especificar IP o rango de IP.
Certificación	Operador del Servicio	1. Todo cerrado excepto. a. Puertos documentados para su respectivo servicio y buen funcionamiento de aplicación. 2. Las reglas se depuran cada tres meses. 3. Los permisos para servicios de administración (ssh, rdp, rpc, etc) no deben provenir de 'any', sino de IP o rango de IP.

4.4.2.6 Control de acceso de los usuarios para uso de la red del MEN.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Define como control de acceso de los usuarios a las redes los siguientes lineamientos: a) Los usuarios del MEN únicamente deben tener permiso de acceso directo a las aplicaciones y bases de datos para cuyo uso están específicamente autorizados. b) Todos los accesos de los usuarios remotos a sistemas y aplicaciones de información del MEN deben estar controlados por medio de autenticación. c) Todas las conexiones remotas que se realicen a sistemas de información del MEN deben ser autenticadas. d) Los puertos empleados para diagnóstico remoto y configuración deben estar controlados de forma segura, deben estar protegidos a través de un mecanismo de seguridad adecuado y un procedimiento	Oficina de tecnología y sistemas de información	

	para asegurar que los accesos lógicos y físicos a estos son autorizados.		

4.4.2.7 Autenticación de usuarios en la red para conexiones externas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Aprobar la autenticación de usuarios remotos bajo una solicitud con su respectivo formato.	Jefe inmediato del colaborador	
	Usar de forma adecuada los recursos de red y de seguir los procedimientos definidos para el acceso a las redes	Todos los colaboradores y terceros del MEN	

4.4.2.8 Accesos al sistema operativo (WINDOWS, LINUX entre otros).

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Asegurar que los medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos deberán contener como mínimo las siguientes características: a) Autenticar usuarios autorizados, de acuerdo con una política definida de control b) de acceso; c) Registrar intentos exitosos y fallidos de autenticación del sistema; d) Emitir alarmas cuando se violan las políticas de seguridad del sistema; e) Suministrar medios adecuados para la autenticación f) Cuando sea apropiado, restringir el tiempo de conexión de los usuarios	Oficina de Tecnología y sistemas de Información	

4.4.2.9 Acceso a los sistemas de información

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES

Evitar el acceso no autorizado a sistemas y aplicaciones	Acceder a los recursos de servicios de información a través de la cuenta de usuario asignada.	Todos los colaboradores y terceros del MEN	
	Permitir el acceso lógico al software de aplicación solo a usuarios autorizados.	Oficina de Tecnología y sistemas de Información	
	Asegurar que el acceso a las aplicaciones y bases de datos sea independiente del acceso al sistema operativo.		

4.4.3 Sistema de gestión de contraseñas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Solicitar la asignación, modificación o revocación de privilegios en los Sistemas de Información del MEN a los usuarios de su dependencia. Existirán privilegios asociados a: b) Usuarios. c) Perfiles, tales como: Administrador, Operador, Usuario Externo, Usuario Interno, Usuario Temporal o Etc. d) Recursos, tales como: Bases de datos, Aplicaciones. o Etc. e) Permisos, tales como: Lectura, Escritura o Control total.	Líderes de procesos, Directores, Jefes de dependencias	
	Asegurar que los sistemas estén diseñados o configurados de tal forma que sólo se acceda a las funciones permitidas.	Oficina de Tecnología y sistemas de Información	
	Asegurar que la información del usuario se creará al darlo de alta por primera vez en alguno de los sistemas afectados, y deberá mantenerse actualizada, registrándose todas aquellas modificaciones que se produzcan en los privilegios de acceso hasta el momento en que se haya causado su baja en todos los sistemas incluidos en el alcance.		

- ✓ Cumplir y acatar las políticas de seguridad de la información.
- ✓ Asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- ✓ Buscar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- ✓ Asegurar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- ✓ Propender que los controles de autenticación cuando fallen lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- ✓ Asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.
- ✓ Asegurar que se inhabilitan las cuentas de manera temporal luego de un número establecido de intentos fallidos de ingreso a los sistemas desarrollados.
- ✓ Asegurar que, si se utiliza la reasignación de contraseñas, únicamente se envíe un enlace o contraseñas temporales a cuentas de correo electrónico previamente registradas en los aplicativos, los cuales deben tener un periodo de validez establecido; se deben forzar el cambio de las contraseñas temporales después de su utilización.
- ✓ Asegurar que, el último acceso (fallido o exitoso) sea reportado al usuario en su siguiente acceso exitoso a los sistemas de información.
- ✓ Asegurar la re-autenticación de los usuarios antes de la realización de operaciones críticas en los aplicativos.
- ✓ Restringir acceso a archivos u otros recursos, a nivel de los aplicativos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
- ✓ Asegurar que periódicamente se revalida la autorización de los usuarios en los aplicativos y se asegura que sus privilegios no han sido modificados.

4.4.4 Uso de programas utilitarios privilegiados

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	Oficina de Tecnología y sistemas de Información	
	Definir el uso de procedimientos de identificación, autenticación y autorización para los programas utilitarios.		
	Separar los programas utilitarios del software de aplicaciones.		
	Limitar el uso de programas utilitarios al número mínimo práctico de usuarios confiables y autorizados.		
	Limitar la disponibilidad de los programas utilitarios, por ejemplo, para la duración de un cambio autorizado.		
	Registrar el uso de los programas utilitarios.		
	Definir y documentar los niveles de autorización para los programas utilitarios.		
	Retirar o deshabilitar todos los programas utilitarios innecesarios.		
	No poner a disposición los programas utilitarios a los usuarios que tengan acceso a aplicaciones en sistemas en donde se requiera la separación de deberes.		

4.4.5 Control de acceso a código fuente de programas

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Evitar el acceso no autorizado a sistemas y aplicaciones	Controlar estrictamente el acceso a los códigos fuente de programas y elementos asociados (tales como diseños, especificaciones, planes de verificación y planes de validación), con el fin de evitar la introducción de funcionalidad no autorizada y para evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual valiosa.	Oficina de Tecnología y sistemas de Información	
	No mantener las librerías de fuentes de programas en los sistemas operativos.		

	Establecer procedimientos para la gestión de los códigos fuente de los programas y las librerías de las fuentes de los programas.		Directorio activo
	Restringir el acceso al personal de soporte a las librerías de las fuentes de los programas.		Directorio activo
	No efectuar la actualización de las librerías de fuentes de programas y elementos asociados, y la entrega de fuentes de programas a los programadores sin que se haya recibido autorización apropiada		
	Mantener en un entorno seguro los listados de programas.		
	Conservar un registro de auditoría de todos los accesos a las librerías de fuentes de programas.		

4. Información de contacto

Cualquier inquietud relacionada con la Guía política de control de acceso, favor remitirla al correo seguridaddigital@mineducacion.edu.co.

5. Revisión de la guía

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

6. Referentes

7.1 Referentes Normativos

Norma ISO 27001

Dominio A.9 Control de acceso

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	Edwar Hidalgo Acosta	**Nombre**	Lina Vannesa Perdomo Castrillón	**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