Guía - Política de Seguridad Física y del Entorno

Tabla de contenido

1 Objetivo

Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información del MEN.

2 Alcance

Lo definido en la presente guía política aplica para el control de acceso físico a las áreas seguras dentro de las cuales se encuentran el centro de datos, centros de cableado, áreas de tesorería, archivo, áreas de recepción y entrega de correspondencia, las cuales deben contar con mecanismos de protección física y ambiental, y controles de acceso adecuados para la protección de la 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.
- **Áreas seguras:** Sitio donde se maneja información sensible o valiosos equipos informáticos, es decir, refugios con los que alcanzar los objetivos del MEN.
- **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.
- **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).

4 Política de seguridad física y del entorno

Directrices

4.1 Áreas seguras

4.1.1 Perímetro de seguridad física

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.	Realizar el inventario y señalizar las áreas seguras de acuerdo con el inventario establecido.	SGA	Inventario de áreas seguras.
	El perímetro de seguridad de las instalaciones del MEN o de las áreas seguras debe ser físicamente sólido (no deben existir aberturas en el perímetro o áreas donde pueda producirse fácilmente una irrupción). Las paredes externas del área deben ser de construcción sólida y todas las puertas que comunican con el exterior deben ser adecuadamente protegidas contra accesos no autorizados, por ejemplo mediante mecanismos de control, vallas, alarmas, cerraduras, etc.		N/A
	Verificar que las puertas y ventanas de las áreas seguras estén cerradas con llave cuando no hay supervisión o están desocupadas.		Bitácoras del equipo de vigías.
	El perímetro de seguridad de las áreas seguras debe contar con vigilancia mediante CCTV, contar con sistemas de control de acceso y debe ser monitoreado por el personal de vigilancia del Ministerio. Nota: Las cámaras no podrán apuntar directamente a la captura de información dentro de estas áreas.		Sistema de Control de Acceso del MEN ST-FT-14 Formato - Ingreso y Salida al Centro de Datos y Centros de Cableado Registros de CCTV
	Todas las puertas de emergencia de un perímetro de áreas seguras deben tener alarma.		N/A
	Mantener organizado e identificado el cableado en los racks de los centros de cableado y centro de datos.	OTSI	Informes de mantenimiento de centros de cableado.

4.1.2 Controles de acceso físico

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Las áreas seguras se deberían proteger mediante controles de entrada, apropiados para asegurar que solamente se permite el acceso a personal autorizado	Todos los puntos de acceso a las instalaciones físicas deberán tener un área de recepción con vigilancia u otro medio para controlar el acceso físico (Personal interno y visitantes) a las instalaciones y debe estar documentado. Nota: Verificar que las áreas seguras e instalaciones, estén ubicadas de manera que se impida el acceso del público.	Subdirección de Gestión Administrativa	Sistema de Control de Acceso del MEN Equipo de vigías. AD-FT-30 Formato - Control de Acceso de Menores de Edad
	El personal de vigilancia debe establecer mecanismos para inspeccionar y examinar los morrales, bolsos, cajas, etc. de los colaboradores o visitantes que ingresen y salen de las instalaciones del MEN. Nota: En algunos puntos de acceso se cuenta con scanner de rayos X.		Contrato de vigilancia. Registros de CCTV
	Registrar en una bitácora o sistema de información el ingreso y retiro de todo equipo de cómputo, servidores, equipos activos de red o cualquier equipo diferente a smartphone; en caso de que estos equipos sean propiedad del Ministerio deberán contar con autorización expresa según sea el caso y de acuerdo con los procedimientos establecidos para tal fin.		Mesa de ayuda de administrativa. Procedimientos
	Deshabilitar o modificar de manera inmediata, los privilegios de acceso físico al MEN y a las áreas seguras, en los eventos de desvinculación o ausencia transitoria, lo anterior de acuerdo con los reportes enviados por la STH y la Subdirección de Contratación. Lo anterior de acuerdo con la Política de Seguridad de los Recursos Humanos.		Solitudes de la STH y Subdirección de Contratación.
	Llevar el registro del acceso a las áreas seguras (centros de cómputo y centros de cableado, entre otros) Nota 1: El centro de cómputo externo se rige por las normas y políticas establecidas por el operador de servicios TIC de collocation. Nota 2: Todo el personal que ingrese al centro de datos y centros de cableado deberá portar identificación visible y presentarla en la puerta de acceso antes de su ingreso (Parel caso de centros de cómputo y centros de cableado interno). Nota 3: Cuando se trate de personal externo al Ministerio deberá estar acompañado	Oficina de Tecnología y Sistemas de Información	ST-FT-14 Formato - Ingreso y Salida al Centro de Datos y Centros de Cableado

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	por quien sea autorizado, éste se hará responsable de la estadía del personal ajeno al Ministerio durante el tiempo que permanezca en las instalaciones.		
	Autorizar el acceso al centro de cómputo, centros de cableado, gabinetes (racks) ya que es restringido este acceso y solo debería ingresar el personal autorizado. Adicionalmente, se debe realizar el monitoreo correspondiente a estos accesos.	Centro de cómputo (Responsable del SGSI OTSI) Centros de cableado (SGA) Racks (operador de servicios TICs)	Solicitud de acceso y autorización de la OTSI en la mesa de ayuda de tecnología.
	Autorizar recibir visitantes en las instalaciones del MEN tanto durante en el horario autorizado como en horarios distintos al autorizado (el autorizado es de 8:00 AM a 5:00 PM de L a V)	Jefes de Dependencia o Coordinador del Grupo correspondiente.	Sistema de Control de Acceso del MEN

4.1.3 Seguridad de oficinas, recintos e instalaciones.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	Borrar la información escrita en los tableros o pizarras al finalizar las reuniones de trabajo. Igualmente, no se deben dejar documentos o notas escritas en los espacios al finalizar las reuniones.	Todos los colaboradores y terceros del MEN	N/A
	Garantizar que los visitantes se encuentren acompañados de un colaborador del MEN, cuando se encuentren en las oficinas o áreas seguras donde se maneje información.		
	Asegurar que los visitantes que requieran permanecer en las oficinas del MEN por periodos superiores a dos (2) días sean presentados al personal de oficina donde permanecerán.		

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Portar su carné o escarapela en un lugar visible mientras permanezca dentro de las instalaciones del MEN.		
	Proteger los dispositivos de almacenamiento de información externos, así como toda información CONFIDENCIAL del MEN, independientemente del medio en que se encuentre, y tenerlos bajo seguridad durante horario no hábil o en horarios en los cuales los colaboradores o terceros responsables no se encuentren en su sitio de trabajo.		N/A
	En ninguna circunstancia, se debe fumar, comer o beber en las áreas seguras.		
	Verificar que no se toman fotografías o grabación de video, en áreas de procesamiento de información o donde se encuentren activos de información que comprometan la seguridad o la imagen del MEN, a menos que esté autorizado.		
	Permanecer acompañados de un colaborador del MEN, cuando se encuentren en las instalaciones o áreas seguras, y portar siempre la escarapela de ingreso en un lugar visible.	Todos los visitantes del MEN	Sistema de Control de Acceso
	Verificar que las edificaciones sean discretas y no den indicio de su propósito, sin señales obvias externas o internas, que identifiquen la presencia de actividades de procesamiento de información.	Subdirección de Gestión Administrativa	Señalización
	Señalizar lo correspondiente al interior de las áreas seguras: (Prohibido tomar fotografías o grabación de video, prohibido, fumar comer o beber, ente otros)		
	Verificar que las instalaciones estén configuradas para evitar que las actividades o información confidenciales sean visibles y audibles desde el exterior. El blindaje electromagnético también se debe considerar apropiado.		N/A
	Asegurar que los directorios y guías telefónicas internas que identifican los lugares de las instalaciones de procesamiento de información confidencial no sean accesibles a ninguna persona no autorizada.		
	Supervisar las actividades de limpieza en las áreas seguras, especialmente: centro de datos y centros de cableado, brindando capitación al personal de limpieza acerca de las precauciones mínimas a seguir durante el proceso de limpieza,	SGA Oficina de Tecnología y	Contrato de mantenimiento y aseo.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	adicionalmente se prohíbe el ingreso de maletas, bolsos u otros objetos que no sean propios de las tareas de aseo.	Sistemas de Información	

4.1.4 Protección contra amenazas externas y ambientales

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes	Proveer las condiciones físicas y medioambientales necesarias como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia, entre otros para certificar la protección y correcta operación de la gestión de la información y de los recursos de la plataforma tecnológica. Estos sistemas se deben monitorear de manera permanente.	Subdirección de Gestión Administrativa	Registro de monitoreo de aires acondicionados.
	Mantener en buen estado la infraestructura física de los centros de cableado, centros de datos del Ministerio, y en general de las áreas seguras, tales como puertas, cerraduras, ventanas, techos, paredes, pisos, aires acondicionados, cielos rasos, pisos falsos, sensores, entre otros.		Planes de mantenimiento correctivo y preventivo.
	Asegurar que el centro de cómputo o de cableado, se encuentre separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones o incendios.		
	Mantener libre de objetos o elementos que no sean propios en la operación en el centro de datos y centros de cableado del Ministerio.	OTSI	
	Elaborar e implementar los planes de contingencia, de emergencia y de continuidad del negocio.	OTSI, SGA y STH	Plan de emergencias del MEN Plan de Contingencia y Continuidad del Negocio.

4.1.5 Trabajo en áreas seguras

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras	Asegurar que las labores de mantenimiento de redes eléctricas, y de datos, dentro del centro de cómputo, sean realizadas acorde con el procedimiento de Gestión de Cambios y por personal idóneo y apropiadamente, autorizado previamente por el comité de cambios; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.	Oficina de Tecnología y Sistemas de Información	Planes Preventivos de Mantenimiento. Registros de Aprobación de Comité de Cambios.
	Asegurar que las labores de mantenimiento para los centros de cableado y/o cuarto eléctricos sean realizadas por personal idóneo y apropiadamente; así mismo, se debe llevar control de la programación de los mantenimientos preventivos, previa autorización de la OTSI.	Subdirección de Gestión Administrativa Oficina de Tecnología y Sistemas de Información	Planes Preventivos de Mantenimiento. Registros de Autorización de la OTSI

4.1.6 Áreas de despacho y carga

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	Señalizar las áreas de cargue y descargue del Ministerio.	Subdirección de Gestión Administrativa	Señalización
	Controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. Los puntos de acceso como el área de entrega y las zonas de carga deberán ser controladas y monitoreadas mediante CCTV.		Sistema de Control de Acceso del MEN Registros de CCTV
	Restringir el acceso al área de despacho y de carga desde el exterior de la edificación únicamente al personal identificado y autorizado.		Sistema de Control de Acceso Bitácora del Equipo de Vigías
	Diseñar el área de despacho y carga de manera que los suministros se puedan cargar y descargar sin que el personal de despacho tenga acceso a otras partes de la edificación.		Planos
	Asegurar las puertas externas de un área de despacho y carga cuando las puertas internas están abiertas.		
	Registrar el material que ingresa de acuerdo con los procedimientos de gestión de activos al entrar al sitio.		Mesa de ayuda de administrativa Procedimiento??
	Inspeccionar y examinar el material que ingresa para determinar la presencia de explosivos, químicos u otros materiales peligrosos, antes de que se retiren del área de despacho y carga.		Bitácora del Equipo de Vigías
	Inspeccionar el material entrante para determinar evidencia de manipulación durante el viaje. Si se descubre esta manipulación, se debería reportar de inmediato al personal de seguridad.		Bitácora del Equipo de Vigías

4.2 Equipos

4.2.1 Ubicación y protección de los equipos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.	Asegurar que la plataforma tecnológica (Hardware, software y comunicaciones) cuente con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.	Oficina de Tecnología y Sistemas de Información.	Informes de seguridad de Hardware, software y comunicaciones.
	Asegurar que los equipos de cómputo de escritorio asignados a los colaboradores cuenten con las condiciones adecuadas para su funcionamiento. Notas: Estos equipos no pueden ser removidos del lugar asignado sin la autorización de la OTSI.		Sistrma Service Manager - CA Mesa de ayuda de tecnología Mesa de ayuda de administrativa
	Proteger la infraestructura de procesamiento de información mediante contratos de mantenimiento y soporte.		Contratos de mantenimiento y soporte.

4.2.2 Servicios de suministro

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Asegurar la protección de los equipos de cómputo contra cortes de luz y otras interrupciones provocadas por fallas en los suministros básicos.	Oficina de Tecnología y Sistemas de Información	Suministro de energía ininterrumpible (UPS) Planta eléctrica
	Los equipos de UPS deben inspeccionarse periódicamente para asegurar que tienen la capacidad requerida y se deben probar de conformidad con las recomendaciones del fabricante o proveedor.		Contrato de mantenimiento de las UPS
	Asegurar que se instalen sistemas de protección eléctrica en el centro de cómputo y comunicaciones de manera que se pueda interrumpir el suministro de energía en caso de emergencia.		Interruptores de emergencia.

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
	Controlar la entrada de equipos electrónicos a los centros de cómputo del MEN.		ST-FT-14 Formato - Ingreso y Salida al Centro de Datos y Centros de Cableado
	Asegurar la operación permanente de los servidores alojados en los centros de cómputo, de igual forma proteger la información almacenada en los sistemas de almacenamiento, para que esté segura y disponible.		Monitoreo de infraestructura y servicios TIC - Spectrum Indicador de disponibilidad
	Los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las salas donde se encuentra el equipamiento, a fin de facilitar un corte rápido de la energía en caso de producirse una situación crítica.	SGA	interruptores de emergencia
	Se debe proveer de iluminación de emergencia en caso de producirse una falla en el suministro principal de energía.		iluminación de emergencia
	Se debe implementar protección contra rayos en todos los edificios y se deben adaptar filtros de protección contra rayos en todas las líneas de comunicaciones externas.		Filtros protección

4.2.3 Seguridad del cableado

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.	Proteger contra interceptación, interferencia o daño el cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información.	Oficina de Tecnología y Sistemas de Información	Plan e informes de mantenimiento preventivo y correctivo.
	Los cables de potencia deben estar separados de los cables de comunicaciones para evitar interferencia.		
	Asegurar que los centros de cableado y/o cuarto eléctrico tengan las condiciones físicas y medioambientales.	Subdirección de Gestión Administrativa	

4.2.4 Mantenimiento de equipos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.	Asegurar que se les efectúe mantenimiento a los equipos adecuadamente con el objeto de garantizar su disponibilidad e integridad continua.	Oficina de Tecnología y Sistemas de Información	Plan e informes de mantenimiento preventivo y correctivo.
	Asegurar el correcto funcionamiento de los equipos de cómputo, concretando tiempos de mantenimiento de los equipos con el operador de Servicios TICs y con los colaboradores.		
	Sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.		
	Se deben mantener registros de todas las fallas supuestas o reales y de todo el mantenimiento preventivo y correctivo.		
	Establecer y supervisar que el mantenimiento se realice de acuerdo con lo definido en el contrato del operador de servicios TICs el cual contempla un mantenimiento preventivo a los servidores del centro de cómputo, por lo menos dos (2) veces al año, de acuerdo con lo definido por la OTSI.		Contrato del operador de Servicios TIC

4.2.5 Retiro de activos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.	Autorizar el retiro de los equipos, la información o el software del MEN. Ningún equipo de cómputo, información o software debe ser retirado del Ministerio sin una autorización formal.	Subdirección de Gestión Administrativa	Mesa de ayuda de administrativa
	Todo movimiento de los equipos, la información o el software del MEN debe ir acompañado de una solicitud a la mesa de ayuda de administrativa, de lo contrario, el activo fijo puede ser retenido por el personal de seguridad.		Mesa de ayuda de administrativa
	Realizar periódicamente inspecciones para detectar el retiro no autorizado de equipos, información o el software del MEN.	Subdirección de Gestión Administrativa Oficina de Tecnología y Sistemas de Información	Registro de inspecciones
	Exigir identificación a aquellas personas que se encuentren trasladando equipos, información o software y estas deben acreditarse como colaboradores del MEN.	Subdirección de Gestión Administrativa Equipo de vigías	Bitácora equipo de vigías.
	Solicitar la asignación de los equipos necesarios para realizar trabajos externos de acuerdo las autorizaciones correspondientes.	Todos los colaboradores del MEN	Mesa de ayuda de administrativa

4.2.6 Seguridad de equipos y activos fuera de las instalaciones

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	Asegurar que los equipos que se encuentran sujetos a traslados físicos fuera del MEN posean pólizas de seguro que cubran los diferentes riesgos que puedan presentar.	Subdirección de Gestión Administrativa	Pólizas
	Asegurar que los equipos portátiles que contengan información clasificada como CONFIDENCIAL o RESERVADA, cuenten con controles de seguridad que garanticen la confidencialidad de la información.	Oficina de Tecnología y Sistemas de Información	Controles criptográficos.
	Asegurar que los equipos portátiles no estén a la vista en el interior de los vehículos. En caso de viaje siempre se debe llevar como equipaje de mano.	Todos los colaboradores y terceros del MEN.	N/A
	Informar inmediatamente a Subdirección de Gestión Administrativa y OTSI en caso de pérdida o robo de un equipo portátil, debe poner la denuncia ante las autoridades competentes y debe hacer llegar copia de esta.		Mesa de ayuda de tecnología Denuncia por perdida o hurto.
	Asegurar con una guaya los equipos portátiles cuando se encuentren desatendidos, dentro o fuera de las instalaciones del MEN.		Registro de entrega del equipo.
	Registrar todos los equipos de cómputo al ingreso y al retirarse de las instalaciones del MEN.		Sistema de Control de Acceso Bitácora del Equipo de Vigías
	Deshabilitar los puertos de transmisión y recepción de infrarrojo y bluetooth para el caso de los equipos que cuentan con estos.		N/A

4.2.7 Disposición segura o reutilización de equipos

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	Realizar la copia de respaldo de la información que se encuentre almacenada en los equipos de cómputo. Cuando un equipo de cómputo sea reasignado o dado de baja, posteriormente, debe ser sometido al procedimiento de borrado seguro de la información y del software instalado, con el fin de evitar pérdida de la información o recuperación no autorizada de la misma.	Oficina de Tecnología y Sistemas de Información	Copias de respaldo de los equipos de cómputo. Registros de borrado seguro de la información y del software instalado.

4.2.8 Equipo de usuario desatendido

CONTROL	DIRECTRICES	ACTORES	SOPORTE A DIRECTRICES
Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.	Asegurar que cuando se ausenta de su puesto de trabajo los equipos desatendidos se les de protección de acuerdo con la política de pantalla limpia y escritorio despejado.	Todos los colaboradores y terceros del MEN	N/A
	Cerrar las sesiones activas cuando hayan terminado su trabajo y bloquear la pantalla cuando se ausente de su puesto de trabajo. Salir de las aplicaciones o servicios de red cuando ya no los necesiten.		N/A

5 Información de contacto

Cualquier inquietud relacionada con la Guía política de seguridad física y del entorno, favor remitirla al correo seguridaddigital@mineducacion.edu.co.

6 Revisión de la guía

Esta guía debe ser revisada por la OTSI y la Subdirección de gestión administrativa como mínimo una vez al año.

7 Referentes

7.2.6.1 Referentes Normativos

- Norma ISO 27001
- Dominio A.11 Seguridad física y del entorno

7.2.6.2 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 -

7.2.6.2.1 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 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