LINEAMIENTO DE USO DE DISPOSITIVOS MÓVILES EN LAS REDES INSTITUCIONALES- SED Referencia: ISO/IEC 27001:2022, control 8.1 (Dispositivos de punto final de usuario)

Sistema de Gestión de Seguridad de la Información
Secretaría de Educación Del Distrito

Versión 1.0
Octubre 2026

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN
BOGOTÁ

Tabla de Contenido

1 INTRODUCCIÓN 7
2 Objetivo 7
3 Alcance 7
4 MARCO LEGAL Y NORMATIVO 8
5 LINEAMIENTOS DE USO DE DISPOSITIVOS MÓVILES 9
6 LINEAMIENTOS DE SEGURIDAD BASADOS EN ISO 27001:2022 9
6.1 LINEAMIENTOS PARA DISPOSITIVOS CORPORATIVOS 9
6.1.1 Inventario y Registro 10
6.1.2 Configuración de Seguridad Obligatoria 10
6.2 LINEAMIENTOS PARA DISPOSITIVOS PERSONALES (BYOD) 11
6.2.1 Principios Generales y Límites de Control 11
6.2.2 Registro y Habilitación de Conectividad 12
6.2.3 Reglas de Uso para Dispositivos Personales 12
6.2.4 Aplicación de Filtrado Web en Dispositivos Personales 13
6.2.5 Recomendaciones de Seguridad para el Usuario 14
6.2.6 Restricciones de Conectividad 14
6.2.7 Soporte Técnico para Dispositivos Personales 14
6.3 AUDITORÍA Y REVISIÓN 15
7 PROCEDIMIENTO ANTE PÉRDIDA O HURTO 15
8 INCUMPLIMIENTO DE LA POLÍTICA 16
9 RESPONSABILIDADES 16

VOCABULARIO

Aplicación corporativa: Software autorizado, licenciado y gestionado por la SED para el cumplimiento de funciones institucionales, incluyendo Microsoft Teams, Outlook, OneDrive for Business, SharePoint y demás herramientas de la suite Microsoft 365, así como cualquier otra solución corporativa que la Entidad adopte oficialmente para comunicaciones, almacenamiento o colaboración (ej., Dexon, según las definiciones de la OTIC).

Aplicación no autorizada: software, herramienta o servicio digital que no ha sido aprobado, licenciado o gestionado por la SED, y cuyo uso en dispositivos corporativos está prohibido. En dispositivos personales, su uso no es controlable por la Entidad.

Auditoría de seguridad: Proceso sistemático y documentado para verificar el cumplimiento de las políticas, lineamientos y controles de seguridad de la información, incluyendo la revisión de configuraciones, registros de actividad y prácticas de los usuarios.

Autenticación: Proceso mediante el cual se verifica la identidad de un usuario, dispositivo o sistema antes de concederle acceso a los recursos de información.

Autenticidad: Principio de seguridad de la información que garantiza que un mensaje, transacción o dato proviene de una fuente legítima y no ha sido falsificado, asegurando que la identidad del emisor es verificable.

Bloqueo automático de pantalla: Función de seguridad que bloquea el acceso a un dispositivo móvil después de un período de inactividad predefinido, requiriendo autenticación para su reactivación.

BYOD (Bring Your Own Device): Práctica que permite a los empleados utilizar sus dispositivos personales (teléfonos inteligentes, tabletas, portátiles) para fines laborales.

Cifrado de dispositivo: Tecnología que convierte la información almacenada en un dispositivo en un formato ilegible sin la clave de descifrado correspondiente, protegiendo los datos en caso de pérdida, hurto o acceso no autorizado.

Confidencialidad: Principio de seguridad de la información que asegura que los datos sean accesibles únicamente por aquellas personas, procesos o sistemas autorizados, impidiendo su divulgación a terceros no autorizados.

Contenedorización: Aislamiento lógico de los datos y aplicaciones corporativas de los personales en un mismo dispositivo, permitiendo la gestión remota del entorno laboral sin afectar la esfera personal del usuario.

Control de acceso: Mecanismo que regula quién puede acceder a qué recursos,

aplicaciones o información, y en qué condiciones, garantizando que solo los usuarios autorizados puedan utilizar los dispositivos y redes institucionales.

Control de aplicaciones (Application Control): Capa de seguridad basada en software que aplica una lista explícita de aplicaciones que se permiten ejecutar en un dispositivo o red, bloqueando aquellas no autorizadas. Ver Matriz de Control de Aplicaciones.

Datos personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables, incluyendo nombre, identificación, domicilio, dirección electrónica, número de teléfono, entre otros.

Dato sensible: Información que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tal como origen racial o étnico, orientación política, convicciones religiosas, pertenencia a sindicatos, datos de salud, vida sexual y datos biométricos.

Disponibilidad: principio de seguridad de la información que garantiza que los sistemas, aplicaciones y datos estén accesibles y operativos cuando los usuarios autorizados los requieran.

Dispositivo corporativo: Equipo electrónico de propiedad de la SED, asignado a un funcionario, contratista o colaborador para el desarrollo de sus funciones institucionales. Incluye teléfonos inteligentes, tabletas y portátiles registrados en el inventario de la Entidad.

Dispositivo móvil: Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria. Ejemplos: teléfonos inteligentes (smartphones), tabletas (tablets) y portátiles (laptops).

Dispositivo personal: Equipo electrónico de propiedad del usuario (funcionario, contratista o colaborador) que puede ser utilizado para fines laborales bajo el esquema BYOD, siempre que cumpla con las condiciones establecidas en este lineamiento.

DLP (Data Loss Prevention): Conjunto de herramientas y prácticas para prevenir la fuga de datos sensibles.

Equipo Técnico de las Políticas de Gobierno y Seguridad Digital: Instancia de gobernanza táctica de la SED, creada mediante la Resolución 001 de 2025, conformada por profesionales de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), la Oficina Asesora de Planeación y la Oficina Asesora de Comunicaciones y Prensa. Sus funciones incluyen la revisión y actualización de políticas de seguridad, la auditoría de cumplimiento, la definición de excepciones, la evaluación de riesgos y la coordinación de la respuesta a incidentes de seguridad de la información**.**

Excepción de filtrado: Autorización temporal y justificada para acceder a una URL, aplicación o categoría web que normalmente estaría bloqueada por las políticas de filtrado. Debe ser aprobada por Seguridad de la Información y tener un tiempo de vigencia definido.

Filtrado web: Conjunto de mecanismos técnicos que controlan y restringen el acceso a sitios web, aplicaciones y contenidos en Internet, basados en categorías, perfiles de usuario y políticas de seguridad predefinidas.

Información corporativa: Todo conjunto de datos, documentos, archivos, bases de datos, comunicaciones y registros generados, procesados o almacenados por la SED en el ejercicio de sus funciones, independientemente de su soporte (impreso, óptico o electrónico).

Información confidencial: Información en poder de la SED cuyo acceso público se prohíbe por mandato constitucional o legal debido a un interés personal jurídicamente protegido. Incluye datos personales, información médica y aquella cuya divulgación constituiría una invasión a la privacidad.

Información reservada: Información pública cuyo acceso se restringe de manera expresa debido a un interés general durante un período determinado y por causas justificadas, como negociaciones en curso o investigaciones de actos ilícitos.

Inspección SSL/TLS (SSL Inspection): Proceso mediante el cual el tráfico web cifrado (HTTPS) es descifrado, inspeccionado y vuelto a cifrar para detectar amenazas, programas malignos o contenido no autorizado, sin comprometer la confidencialidad de la información.

Integridad: principio de seguridad de la información que garantiza que los datos no han sido alterados, modificados o destruidos de manera no autorizada, asegurando que la información es exacta y completa.

Lineamiento: Conjunto de directrices, reglas y procedimientos que orientan la implementación de políticas de seguridad en áreas específicas, desarrollando y detallando los controles establecidos en los documentos normativos de nivel superior.

Log / Registro de actividad: Archivo electrónico que documenta eventos, transacciones y actividades realizadas en sistemas, redes o dispositivos, utilizado para auditoría, monitoreo y análisis de incidentes de seguridad.

Matriz de Control de Aplicaciones: Tabla que define la acción a tomar (Permitir, Bloquear o Monitorear) sobre cada categoría de aplicación (p. ej., Botnet, P2P, Proxy, Social Media, etc.), diferenciada por perfil de usuario (Estándar, VIP, Colegios, Invitado/BYOD).

Matriz de Control Filtrado WEB: Tabla que define la acción a tomar (Permitir,

Bloquear o Monitorear) sobre cada categoría web y subcategoría (p. ej., Alcohol, Juego, Redes Sociales, etc.), diferenciada por perfil de usuario.

MDM (Mobile Device Management): Solución tecnológica que permite a las organizaciones gestionar, monitorear y asegurar dispositivos móviles corporativos, incluyendo la aplicación de políticas de seguridad, configuración remota, instalación de aplicaciones y borrado de datos, independientemente del sistema operativo (Windows, macOS, iOS, Android) y sin necesidad de que los dispositivos estén registrados en un dominio de Active Directory.

Monitoreo de red: Proceso continuo de supervisión del tráfico que circula por la red institucional con fines de seguridad, detección de amenazas y cumplimiento normativo. No implica la inspección del contenido del dispositivo personal.

MSPI (Modelo de Seguridad y Privacidad de la Información): Marco implementado por la SED para gestionar la seguridad y privacidad de la información, alineado con los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y el Modelo de Gestión de Seguridad y Privacidad de la Información para entidades del Estado colombiano.

NGFW (Next-Generation Firewall): Dispositivo de seguridad de red que evoluciona más allá de los cortafuegos tradicionales, combinando filtrado de tráfico estándar con inspección profunda de paquetes, control basado en aplicaciones, prevención de intrusiones integrada e inteligencia de amenazas en tiempo real.

No repudio: principio de seguridad de la información que garantiza que un usuario no pueda negar haber realizado una acción específica, como el envío de un mensaje o la modificación de un dato, proporcionando evidencia verificable de las transacciones.

Perfil de filtrado web: Conjunto predefinido de políticas de acceso a Internet y aplicaciones, asignado a un grupo de usuarios según su rol, función o ubicación. Los perfiles definidos en la SED son: Estándar, VIP, Colegios e Invitado/BYOD.

Política de filtrado web: conjunto definido de acciones a tomar (permitir, bloquear o monitorear) sobre un grupo de categorías web y aplicaciones, establecido por la Entidad para proteger la red, la información y los usuarios.

Principio de proporcionalidad: principio que establece que las restricciones y controles aplicados sobre los usuarios y dispositivos deben ser proporcionales al nivel de riesgo y a la finalidad perseguida, sin exceder lo necesario para proteger la información institucional.

Red institucional: Infraestructura de telecomunicaciones propiedad de la SED, que incluye redes alámbricas, inalámbricas (WiFi) y conexiones VPN, diseñada para facilitar las labores institucionales de los usuarios autorizados.

SGSI (Sistema de Gestión de Seguridad de la Información): Enfoque sistemático, documentado y basado en riesgos que las organizaciones utilizan para establecer, implementar, operar, monitorear y mejorar su seguridad, con el objetivo de proteger los activos de información garantizando su confidencialidad, integridad y disponibilidad.

SSL Bypass: Lista de dominios o categorías web exentas de la inspección SSL/TLS, establecida para proteger la privacidad legal de los usuarios en áreas como banca, salud, correo electrónico personal y autenticación gubernamental.

URL (Uniform Resource Locator): Secuencia de caracteres utilizada para nombrar y localizar recursos en Internet, como páginas web, archivos o servicios.
Uso aceptable: Conjunto de reglas y condiciones que definen los usos permitidos y prohibidos de los recursos tecnológicos, dispositivos e información de la Entidad, estableciendo las responsabilidades de los usuarios.

UTM (Unified Threat Management): Dispositivo de seguridad que integra múltiples funciones de protección en una sola solución, incluyendo firewall, antivirus, filtrado web, prevención de intrusiones y control de aplicaciones.

VPN (Virtual Private Network): Tecnología que crea una conexión segura y cifrada a través de Internet, permitiendo a los usuarios acceder a la red institucional de forma remota como si estuvieran conectados directamente.

Webmail: Servicio de correo electrónico accesible a través de un navegador web sin necesidad de un cliente de correo dedicado. Ejemplos: Gmail, Outlook.com, Yahoo Mail.

Zero-day: Vulnerabilidad de seguridad desconocida para el fabricante o desarrollador, para la cual no existe un parche o actualización disponible en el momento de su descubrimiento, siendo explotada por atacantes antes de que se pueda mitigar.

1 INTRODUCCIÓN

La Secretaría de Educación del Distrito (SED) reconoce que los dispositivos móviles son herramientas esenciales para la operación eficiente de la entidad. Sin embargo, su uso, tanto de dispositivos corporativos como personales (BYOD), introduce riesgos significativos para la seguridad de la información.

La presente política actualiza los lineamientos para el uso seguro de estos dispositivos, alineándose con los estándares internacionales para garantizar la protección de los activos de información de la SED.

Esta política se fundamenta en los controles de la norma ISO/IEC 27001:2022, específicamente en el Control A.8.1 - Dispositivos de punto final de usuario como eje principal para la gestión de la seguridad de los dispositivos, y en el Control A.5.10 - Uso aceptable de la información y otros activos asociados para definir las reglas de uso responsable de los activos de información.

El presente lineamiento se desarrolla en el marco del Macroproyecto 6 del Plan Estratégico de Tecnologías de la Información (PETI) de la Secretaría de Educación del Distrito, y se constituye como un instrumento técnico de los proyectos PRY-29 "Fortalecer la seguridad digital del PETI" y PRY-30 "Fortalecer el servicio de conectividad", que desarrollan las estrategias definidas por la Entidad para la modernización, seguridad y resiliencia de su infraestructura tecnológica.

2 OBJETIVO

Establecer las condiciones, obligaciones y lineamientos para la gestión, acceso y uso seguro de dispositivos móviles (corporativos y personales) que se conecten a las redes institucionales o que almacenen o procesen información de la SED, con el fin de proteger la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información, en cumplimiento del marco legal y normativo aplicable.

El presente lineamiento se constituye como un instrumento técnico de los proyectos PRY-29 "Fortalecer la seguridad digital del PETI" y PRY-30 "Fortalecer el servicio de conectividad", en el marco del Macroproyecto 6 del Plan Estratégico de Tecnologías de la Información (PETI) de la Secretaría de Educación del Distrito, asegurando la trazabilidad y articulación del portafolio de proyectos de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC).

3 ALCANCE

Este lineamiento aplica a todo el personal de la SED (servidores públicos, contratistas, pasantes y colaboradores) que utilice dispositivos móviles para fines laborales, así como al personal técnico encargado de su configuración y soporte.

4 MARCO LEGAL Y NORMATIVO

Además del marco legal colombiano vigente (Ley 1273 de 2009, Ley 1437 de 2011, Ley 527 de 1999, Ley 1712 de 2014, Ley 1581 de 2012, Ley 1098 de 2006, Decreto 1078 de 2015, Decreto 1008 de 2018, Resoluciones 1944 y 1945 de 2016), esta política se fundamenta en los siguientes referentes legales y normativos:

Marco Legal Nacional:

- **Ley 2489 de 2025:** "Por medio de la cual se establecen lineamientos para la creación y fortalecimiento de entornos digitales seguros para niños, niñas y adolescentes y se dictan otras disposiciones". Esta ley establece la obligación de las entidades públicas y privadas de implementar mecanismos técnicos y administrativos para prevenir el acceso de menores a contenidos nocivos en entornos digitales, así como la responsabilidad de las instituciones educativas en la protección de los estudiantes en el uso de dispositivos y plataformas tecnológicas.
- **Ley 2564 de 2026:** “Por medio de la cual se establecen medidas de prevención, protección y atención frente a la violencia en el entorno digital y se dictan otras disposiciones”. Esta ley tipifica conductas como el grooming, ciberacoso, sexting, sextorsión, stalking y happy slapping , y establece que las conductas constitutivas de violencia digital contra niños, niñas y adolescentes en entornos escolares activarán la ruta de atención integral para la convivencia escolar conforme a la normatividad vigente . En consecuencia, respalda las restricciones de conectividad y filtrado web implementadas por la SED, así como la obligación de activar los protocolos de reporte y atención ante conductas indebidas detectadas en las redes inalámbricas institucionales.
- **Decreto Reglamentario de 2026:** Norma que desarrolla la Ley 2489 de 2025, estableciendo los lineamientos específicos para la implementación de entornos digitales seguros en las Instituciones Educativas, incluyendo la obligación de filtrar contenidos, reportar incidentes y capacitar a la comunidad educativa en seguridad digital.
- **Ley 1098 de 2006 (Código de Infancia y Adolescencia):** Establece el interés superior del menor como principio rector y la protección integral de los derechos de los niños, niñas y adolescentes, incluyendo su protección en entornos digitales.
- **Ley 1581 de 2012:** "Por la cual se dictan disposiciones generales para la protección de datos personales" y su Decreto Reglamentario 1377 de 2013.
- **Ley 1712 de 2014:** "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- **Resolución 1944 de 2016:** "Por medio de la cual se adopta la Política de Seguridad de la Información de la Secretaría de Educación del Distrito."
- **Decreto 0385 de 2026:** "Por el cual se establecen los lineamientos para la aplicación del principio de privacidad desde el diseño y por defecto en los servicios digitales de las entidades públicas del orden nacional y territorial".

Este decreto establece la obligación de las entidades públicas de incorporar medidas de protección de datos personales desde la concepción de los servicios digitales y de aplicar, por defecto, las configuraciones más restrictivas para la privacidad de los ciudadanos.

- **Resolución 001 de 2025:** "Por la cual se crea el Equipo Técnico de las Políticas de Gobierno y Seguridad Digital como apoyo al Comité Institucional de Gestión y Desempeño, se derogan los artículos 5 y 6 de la Resolución 1395 de 2019". Esta resolución unifica los equipos técnicos de Gobierno Digital y Seguridad Digital en una sola instancia, a cargo de la OTIC, eliminando la referencia a la Resolución 1945 de 2016.

Marco Normativo Internacional:

- **ISO/IEC 27001:2022 - Anexo A.8.1 (Dispositivos de punto final de usuario):** Establece los requisitos para proteger la información almacenada, procesada o accesible a través de dispositivos de punto final de usuario.
- **ISO/IEC 27001:2022 - Anexo A.5.10 (Uso aceptable de la información y otros activos asociados):** Define la necesidad de establecer, documentar e implementar reglas para el uso aceptable y los procedimientos de manejo de la información y otros activos asociados.
- **ISO/IEC 27001:2022 - Anexo A.8.23 (Filtrado web):** Establece los requisitos para controlar el acceso a sitios web externos para reducir la exposición a contenido malicioso.
- **ISO/IEC 27002:2022:** Guía de implementación para los controles del Anexo A.

5 LINEAMIENTOS DE USO DE DISPOSITIVOS MÓVILES

La SED establecerá controles basados en el nivel de riesgo para garantizar que el uso de dispositivos móviles no comprometa la seguridad de la información. Se priorizará el uso de recursos corporativos y se aplicarán medidas proporcionales al tipo de dispositivo. Todo el personal debe conocer y cumplir con las reglas de uso aceptable definidas en esta política.

6 LINEAMIENTOS DE SEGURIDAD BASADOS EN ISO 27001:2022

Los presentes lineamientos de seguridad se fundamentan en la norma ISO/IEC 27001:2022 y en el principio de "Privacidad desde el Diseño y por Defecto" establecido en el Decreto 0385 de 2026, garantizando que los controles de seguridad implementados protejan la información institucional sin vulnerar el derecho a la intimidad de los usuarios.

6.1 LINEAMIENTOS PARA DISPOSITIVOS CORPORATIVOS

Los dispositivos móviles propiedad de la SED son de uso exclusivo para fines

laborales y están sujetos a controles de seguridad integrales.

6.1.1 Inventario y Registro

Todo dispositivo corporativo debe estar registrado en el inventario de activos de la SED, incluyendo:

- Dirección MAC e IMEI
- Asignatario del dispositivo
- Clasificación de la información que procesará
- Fecha de asignación y estado
- Sistema Operativo y Versión
- Antivirus Actualizado

6.1.2 Configuración de Seguridad Obligatoria

Se debe implementar una configuración de seguridad que incluya:

- **Cifrado del dispositivo:** Activado por el personal de soporte durante la configuración inicial.
- **Bloqueo automático de pantalla:** Configurado con un tiempo máximo de inactividad de 2 minutos.
- **Mecanismo de acceso robusto:** Contraseña mayor a 8 caracteres, patrón complejo (mínimo 7 puntos de contacto) o huella digital.
- **Antivirus/Antimalware:** Software instalado y configurado para actualizaciones automáticas.
- **Actualizaciones:** Las actualizaciones del sistema operativo y aplicaciones autorizadas deben ser gestionadas de forma centralizada por la OTIC a través de las herramientas de gestión de dispositivos (MDM/UEM) que la Entidad implemente para tal fin. En ausencia de dichas herramientas, la OTIC deberá establecer procedimientos alternativos que garanticen la actualización oportuna de los dispositivos corporativos, considerando las limitaciones técnicas de cada entorno (p. ej., colegios sin dominio).
- **Restricción de software:** Solo se permitirá la instalación de aplicaciones aprobadas por la SED.
- **Filtrado Web:** todo el tráfico de Internet será filtrado mediante las herramientas de la SED, conforme a la clasificación de perfiles (Estándar, VIP, Colegios, Invitado/BYOD) y a las matrices de control de aplicaciones y categorías web definidas en el Lineamiento de Filtrado Web de la Entidad.

Nota para colegios: La OTIC definirá un plan de implementación progresiva para la gestión centralizada de dispositivos en los colegios, priorizando las sedes con mayor número de equipos y evaluando la viabilidad técnica de las soluciones MDM disponibles. Mientras tanto, los rectores y directores de las Instituciones Educativas Distritales (IED) serán responsables de garantizar que los dispositivos asignados cumplan con las políticas de seguridad establecidas, apoyándose en los procedimientos documentados por la OTIC.

6.2 LINEAMIENTOS PARA DISPOSITIVOS PERSONALES (BYOD).

La SED reconoce que los dispositivos personales son propiedad de los usuarios y, por lo tanto, la entidad tiene un control y visibilidad limitados sobre estos. El alcance de la SED sobre dispositivos personales se limita a:

1. La conectividad a la red institucional.
2. La protección de la información corporativa a la que se accede.
3. La aplicación de controles de filtrado web sobre el tráfico que se origina desde estos dispositivos.

6.2.1 Principios Generales y Límites de Control

La SED no tiene facultad para:

- Realizar inventario de los dispositivos como activos de la SED.
- Monitorear, auditar o controlar el dispositivo en su totalidad.
- Exigir la instalación de software de gestión o monitoreo que afecte el uso personal del dispositivo.
    - Excepción para entornos BYOD gestionados con soluciones de protección de aplicaciones (p. ej., Microsoft Intune MAM-WE): En estos casos, la instalación de un agente (como Company Portal para Android) es necesaria exclusivamente para autenticar el acceso a las aplicaciones corporativas y permitir la aplicación de políticas de protección de datos a nivel de aplicación, sin que ello implique la gestión, monitoreo o afectación del contenido personal del dispositivo. Para dispositivos iOS, este agente puede no ser requerido.
- Restringir el uso de aplicaciones personales.
- Exigir configuraciones de seguridad que afecten el ámbito personal del dispositivo.

El control de la SED se ejerce exclusivamente sobre:

1. El tráfico de red que se origina desde el dispositivo hacia la red institucional.
2. El acceso a la información institucional a través de las aplicaciones corporativas.
3. Las condiciones de uso de las aplicaciones corporativas (Microsoft 365, Teams, OneDrive, SharePoint, etc.), sobre las cuales la SED tiene control total.

Aplicación del Principio de Privacidad desde el Diseño y por Defecto

En cumplimiento del Decreto 0385 de 2026 y del principio de "Privacidad desde el Diseño y por Defecto" (Privacy by Design and by Default), la SED garantiza que los servicios digitales que interactúan con información institucional incorporen medidas de protección de datos desde su concepción. En el contexto de BYOD, este principio se materializa mediante las siguientes acciones:

- Configuraciones forzadas en aplicaciones corporativas: Todo acceso a las aplicaciones corporativas (Microsoft 365, Teams, OneDrive, SharePoint) desde dispositivos personales forzará configuraciones de seguridad mínimas, independientemente de la configuración del dispositivo. Estas configuraciones incluyen, sin limitarse:
    - Autenticación multifactor (MFA) obligatoria: Se implementará de acuerdo con el plan de licenciamiento de Microsoft 365 contratado por la SED, utilizando las capacidades disponibles (Security Defaults para planes básicos, o políticas de acceso condicional para planes que incluyan Microsoft Entra ID P1/P2, como A3/A5 o Business Premium).
    - Políticas de acceso condicional basadas en el riesgo.
    - Restricción de descarga y almacenamiento local de información corporativa.
    - Bloqueo de copia, impresión o reenvío de información sensible.
    - Caducidad de sesiones por inactividad.

- Aislamiento de información corporativa: La información institucional a la que se accede desde dispositivos personales será gestionada exclusivamente a través de las aplicaciones corporativas, garantizando que no sea almacenada localmente en el dispositivo personal, en cumplimiento de la prohibición establecida en el literal a) de la sección 6.2.3.

- **Protección de datos personales:** La SED garantiza que el control ejercido sobre las aplicaciones corporativas no vulnera el derecho a la intimidad del usuario, dado que no implica acceso, monitoreo o auditoría del contenido personal del dispositivo, en cumplimiento de la Ley 1581 de 2012 y el Decreto 0385 de 2026.

6.2.2 Registro y Habilitación de Conectividad

Para efectos de control de acceso a la red institucional:

- El usuario debe diligenciar la solicitud de habilitación a través de la OTIC.
- Debe proporcionar la dirección MAC del dispositivo para su registro en el sistema de control de acceso.
- Debe aceptar formalmente los términos de este lineamiento y del **Lineamiento de Filtrado Web**[1], reconociendo que el acceso a la red implica la aceptación de las condiciones establecidas.
- La autorización debe ser aprobada por el jefe inmediato del solicitante

6.2.3 Reglas de Uso para Dispositivos Personales

a) Prohibición de Almacenamiento de Información Corporativa: Queda estrictamente prohibido almacenar información de la SED, incluyendo

[1] https://educacionbogota.edu.co/portal_institucional/sites/default/files/inline-files/2022/Lineamientos%20de%20Filtrado%20WEB.pdf

documentos, bases de datos, correos electrónicos, fotografías o cualquier otro activo de información, en el dispositivo personal. La información institucional solo podrá ser consultada y almacenada a través de aplicaciones corporativas sin ser descargada o guardada localmente.

b) Prohibición de Envío de Información Sensible: No se debe enviar información clasificada como confidencial, reservada o sensible a través de aplicaciones de mensajería personal (WhatsApp, Telegram, etc.) ni a cuentas de correo personales.

c) Uso de Canales Corporativos: Para cualquier comunicación oficial, el usuario debe utilizar exclusivamente las herramientas corporativas provistas, licenciadas y gestionadas por la SED, tales como Microsoft Teams, correo institucional, OneDrive, SharePoint y demás aplicaciones de la suite Microsoft 365, así como cualquier otra solución corporativa que la Entidad adopte oficialmente para estos fines (ej., plataformas de mensajería, almacenamiento o colaboración aprobadas por la OTIC).

d) Responsabilidad del Usuario**:** El usuario es el único responsable de la seguridad de su dispositivo personal y de las acciones realizadas a través de él. La SED no asume responsabilidad por daños, pérdida de información personal o vulnerabilidades en el dispositivo del usuario.

Estas configuraciones son aplicadas por la SED a nivel de las aplicaciones corporativas y no implican la instalación de software en el dispositivo personal ni el acceso al contenido personal del usuario.

6.2.4 Aplicación de Filtrado Web en Dispositivos Personales

Para garantizar la protección de la red institucional y la información de la SED, todo el tráfico web originado desde dispositivos personales autorizados estará sujeto a los controles de filtrado web definidos en el Lineamiento de Filtrado Web[2] de la Entidad, en cumplimiento del Control A.8.23 de ISO 27001:2022.

La asignación del perfil de filtrado web para dispositivos personales se realizará de acuerdo con el tipo de usuario autorizado:

Tipo de Usuario	Perfil de Filtrado Aplicable	Descripción
Contratistas y colaboradores autorizados	Perfil Estándar	Aplica a usuarios que, desempeñando funciones laborales equivalentes a las de un funcionario de planta, requieren acceso a los mismos recursos y aplicaciones corporativas para el cumplimiento de sus funciones.
Invitados y visitantes	Perfil Invitado / BYOD	Aplica a usuarios externos que requieren acceso temporal o limitado a la red institucional, con restricciones adicionales según lo definido en el Lineamiento de Filtrado

[2] https://educacionbogota.edu.co/portal_institucional/node/9714

Tipo de Usuario	Perfil de Filtrado Aplicable	Descripción
		Web.

La implementación de los mecanismos de filtrado, inspección SSL/TLS, excepciones, monitoreo y registro se regirá estrictamente por lo establecido en los Capítulos 9 y 10 del Lineamiento de Filtrado Web, sin perjuicio de las disposiciones particulares aplicables al perfil BYOD.

Nota: La SED **no monitorea ni audita el contenido del dispositivo personal**, limitándose al análisis del tráfico que se origina desde este hacia la red institucional, en cumplimiento del derecho a la privacidad y la protección de datos personales.

6.2.5 Recomendaciones de Seguridad para el Usuario

La SED recomienda, sin carácter obligatorio, que los usuarios que accedan a la red institucional desde dispositivos personales consideren:

- Activar el cifrado del dispositivo si está disponible.
- Contar con un sistema operativo actualizado.
- Utilizar un mecanismo de acceso (contraseña, patrón o biometría).
- Instalar un antivirus actualizado.
- No utilizar redes WiFi públicas no seguras para acceder a la información institucional.

6.2.6 Restricciones de Conectividad

- La SED podrá bloquear el acceso a la red de cualquier dispositivo personal que evidencie un uso inadecuado o que infrinja las normas de uso aceptable o los lineamientos de filtrado web.
- El soporte técnico de la SED no brindará asistencia ni mantenimiento a dispositivos personales, limitándose a proporcionar la conectividad de red.

6.2.7 Soporte Técnico para Dispositivos Personales

La SED, a través de la OTIC y la Mesa de Soluciones TIC, no brindará soporte técnico ni mantenimiento sobre dispositivos personales (BYOD), incluyendo, pero sin limitarse a:

- Instalación o configuración de software, sistemas operativos o aplicaciones.
- Resolución de problemas de hardware o conectividad interna del dispositivo.
- Actualización de controladores, parches de seguridad o antivirus.
- Recuperación de información almacenada en el dispositivo.
- Configuración de cuentas de correo o aplicaciones personales.

El alcance del soporte de la SED sobre dispositivos personales se limitará exclusivamente a:

- Garantizar que los medios de conexión a la red institucional (puntos de acceso WiFi, puertos de red, VPN) se encuentren operativos.
- Verificar que el dispositivo esté correctamente registrado en el sistema de control de acceso.
- Proporcionar la información necesaria para que el usuario pueda configurar su dispositivo según los requisitos de conectividad definidos por la OTIC.

En consecuencia, el usuario es el único responsable de:

- La instalación, configuración y actualización de su dispositivo personal.
- La resolución de cualquier problema técnico que afecte el funcionamiento de su equipo.
- La implementación de las medidas de seguridad recomendadas en el presente lineamiento.
- Las consecuencias derivadas del mal funcionamiento, pérdida o hurto de su dispositivo personal, así como de la exposición de información institucional almacenada en él en violación de la prohibición establecida en el literal a) de la sección 6.2.3.

6.3 AUDITORÍA Y REVISIÓN

La OTIC a través del Equipo de Seguridad Digital podrán realizar auditorías periódicas para verificar el cumplimiento de esta política en:

- Dispositivos corporativos: verificación directa de configuraciones.
- Dispositivos personales: Verificación del cumplimiento de reglas de uso aceptable a través de mecanismos de monitoreo de red. La SED no monitorea ni audita el contenido del dispositivo personal, limitándose al tráfico que se origina desde este hacia la red institucional.

El incumplimiento será sancionado conforme al Capítulo 8.

7 PROCEDIMIENTO ANTE PÉRDIDA O HURTO

- **Dispositivos Corporativos:** El usuario debe reportar de inmediato la pérdida o el hurto a la Mesa de Soluciones TIC (soportesed@educacionbogota.edu.co). La OTIC procederá a bloquear el acceso del dispositivo a la red y ejecutará el borrado remoto de la información institucional en caso de ser posible.
- **Dispositivos Personales:** El usuario debe reportar la pérdida o hurto para que la SED bloquee el acceso del dispositivo a la red. La SED no tiene capacidad de borrado remoto en dispositivos personales, por lo que el usuario es responsable de las consecuencias de la exposición de información institucional si incumple la prohibición de almacenar información corporativa.

8 INCUMPLIMIENTO DE LA POLÍTICA

El uso inadecuado o el incumplimiento de esta política será considerado una falta grave, dando lugar a procesos disciplinarios y/o legales según lo establecido en el Código Disciplinario Único (Ley 1437 de 2011), el Código Penal (Ley 1273 de 2009) y demás normativa aplicable. El usuario autorizado será responsable de las acciones incorrectas realizadas a través de su dispositivo.

9 RESPONSABILIDADES

- Jefe de la OTIC:
    - Aprobar y emitir formalmente el presente lineamiento en el marco del Subsistema de Gestión de Seguridad y Privacidad de la Información (SGSPI) y el Sistema de Gestión de Calidad (SGC) de la SED.
    - Gestionar y priorizar los recursos presupuestales y tecnológicos necesarios para la sostenibilidad de las plataformas de conectividad institucional y seguridad perimetral, en articulación con el portafolio del PETI 2024-2027 (Macroproyecto 6: Proyectos PRY-29 y PRY-30).
    - Liderar la articulación estratégica del lineamiento ante el Comité de Gestión y Desempeño Institucional, la Alta Dirección y las dependencias de la entidad.
    - Aprobar las actualizaciones periódicas de este instrumento propuestas por el Equipo Técnico de las Políticas de Gobierno y Seguridad Digital.

ROLES DESIGNADOS

Rol	Responsabilidad
Mesa de Soluciones / Administrador de Seguridad Perimetral	Gestión de accesos regulares (MAC, FSSO/Portal Cautivo) – proceso 12-PD-017.
Oficial de Seguridad de la Información	Evaluación de solicitudes de acceso, excepciones justificadas y reglas de privacidad.
Líder del Equipo de Infraestructura y Mesa de Soluciones	Gestión de inventarios y asignación técnica (12-PD-025, 12-PD-030).
Equipo de Estrategia y Gobierno Digital	Articulación técnica de proyectos PETI; documentación y divulgación (PRY-25).
Oficial de Seguridad Informática	Configuración técnica de seguridad en M365 (Conditional Access, Intune MAM-WE).

- Equipo Técnico de las Políticas de Gobierno y Seguridad Digital (ETPGSD):

Conformado por profesionales de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) y otras dependencias de la SED, conforme a la Resolución 001 de 2025 y las disposiciones vigentes sobre gobierno digital será responsable de:

- Revisar y actualizar el presente lineamiento, garantizando su alineación con la normativa vigente y los estándares internacionales.
- Auditar el cumplimiento de las disposiciones aquí establecidas en los dispositivos corporativos y en el tráfico de red de dispositivos personales.
- Certificar los niveles de seguridad implementados y proponer mejoras continuas.
- Asegurar la alineación con los controles A.8.1, A.5.10 y A.8.23 de ISO 27001, así como con la Ley 2489 de 2025, su Decreto Reglamentario de 2026 y el Decreto 0385 de 2026.
- Coordinar la respuesta ante incidentes de seguridad que involucren la exposición de niños, niñas y adolescentes a contenidos nocivos, así como la vulneración de datos personales.
- Aprobar las excepciones a los bloqueos de filtrado web conforme al Capítulo 14 del Lineamiento de Filtrado Web, previa evaluación técnica del Oficial de Seguridad de la Información.
- Evaluar los riesgos asociados al uso de dispositivos móviles y proponer acciones de mitigación en el Plan de Tratamiento de Riesgos.

- Usuarios (Personal Institucional): Cumplir con todos los lineamientos (uso aceptable, configuración, reporte de novedades), hacer un uso responsable de los dispositivos y proteger la información de la SED.

MILENA DEL PILAR SANDOVAL GÓMEZ
Jefe Oficina de Tecnologías de la Información y las Comunicaciones - OTIC

Elaborado:	Juan Carlos Parra Moreno Oficial de Seguridad Informática - OTIC	
Revisado:	Henry Alexander Moyan Oficial de Seguridad Información – OTIC	
Revisado:	Jasson Smith Castro León Profesional Especializado – OTIC	
Revisado:	Luz Dary Vargas Suarez Profesional Especializado – OTIC	
Revisado:	Stephany Grey Suárez Galván Contratista – OTIC	