ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

POLÍTICA DE USO DE DISPOSITIVOS MÓVILES EN LAS REDES INSTITUCIONALES - SED.

SECRETARÍA DE EDUCACIÓN DEL DISTRITO

BOGOTÁ – COLOMBIA

2021

Versión 1.0

Av. Eldorado No. 66 – 63
PBX: 324 10 00 Fax: 315 34 48
Código postal: 111321
www.educacionbogota.edu.co
Información: Línea 195

BOGOTÁ

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE EDUCACIÓN

Contenido

1. INTRODUCCIÓN 3

2. OBJETIVO 3

3. ALCANCE 4

4. MARCO LEGAL 4

5. GLOSARIO 5

6. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES 7

7. LINEAMIENTOS PARA EL USO DE DISPOSITIVOS MOVILES Y REDES INSTITUCIONALES 8

7.1 LINEAMIENTOS DE SEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES QUE ACCEDAN A LA INFORMACIÓN DE LA SED A TRAVÉS DE SUS REDES INSTITUCIONALES. 8

7.1.1 Para niveles Central y Local 8

7.1.2 Para Nivel Institucional 10

7.2 LINEAMIENTOS DE SEGURIDAD PARA EL PERSONAL TÉCNICO ENCARGADO DE CONFIGURAR LOS DISPOSITIVOS MÓVILES (SOPORTE SED). 10

7.3 AUDITORÍA Y REVISIÓN DE LA POLÍTICA DE USO DE DISPOSITIVOS MÓVILES EN LAS REDES INSTITUCIONALES DE LA SED. 10

8. PÉRDIDA DEL DISPOSITIVO 11

9. INCUMPLIMIENTO DE LA POLÍTICA 11

10. RESPONSABILIDADES 11

1. INTRODUCCIÓN

El presente documento de POLÍTICA DE USO DE DISPOSITIVOS MÓVILES EN LA REDES INSTITUCIONALES - SED se adelanta con el fin de dar cumplimiento al tratamiento y protección, preservación y aseguramiento de la integridad, confidencialidad y disponibilidad definidos para los activos de información.

Teniendo en cuenta los avances tecnológicos de software y hardware en los dispositivos móviles, se considera directamente proporcional el nivel de riesgo, de adulteración o pérdida que puede llegar a tener la información almacenada en las bases de datos de la institución.

Así mismo es necesario precisar que si bien los dispositivos móviles, son reconocidos como útiles herramientas en casos de emergencia, también pueden llegar a constituirse es un distractor que impide el desarrollo normal de las labores cumpliendo estándares de seguridad, eficiencia y calidad.

Para el uso de dispositivos móviles como equipos portátiles, teléfonos celulares, tabletas, entre otros, la Secretaría de Educación del Distrito (SED) debe implementar controles de acceso, técnicas criptográficas para cifrar la información crítica almacenada en estos, mecanismos de respaldo de la información que contienen y los demás que se consideren necesarios y pertinentes para garantizar la seguridad de la información.

2. OBJETIVO

Establecer las condiciones para el manejo de los dispositivos móviles, únicamente los pertenecientes al inventario de la entidad, que acceden a información de la Secretaría de Educación del Distrito a través de sus redes institucionales, y velar por el uso responsable de éstos por parte de sus funcionarios y personal adyacente.

3. ALCANCE

Esta política aplica para todo el personal de la Secretaría de Educación del Distrito (SED) con acceso a información a través de dispositivos móviles, y para el personal encargado (técnicos de Mesa de Soluciones de la entidad) de configurar de manera segura los dispositivos móviles al servicio de la entidad.

4. MARCO LEGAL

- **Ley 1273 de 2009:** "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- **Ley 1437 de 2011:** (Nuevo Código Disciplinario Único), en lo relacionado con la incorporación de las Tecnologías de la Información y las Comunicaciones en la administración pública.
- **Decreto 1078 de 2015:** "por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
- **Decreto 1008 de 2018**: "por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
- **Decreto-ley 1421 de 1993**: "Por el cual se dicta el régimen especial para el Distrito Capital de Santafé de Bogotá".
- **Ley 527 de 1999**: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."
- **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."
- **Resolución 1945 de 2016**: "Por medio de la cual se crea el Comité Técnico del Subsistema de Seguridad de la Información de la Secretaría de Educación del Distrito y se definen los roles y responsabilidades."

A partir de la adopción del Modelo Integrado de Planeación y Gestión y la política de Seguridad Digital en la SED, se realizará seguimiento, gestión, monitoreo y/o auditoría de esta política con base a la norma **ISO 27002:2013** bajo la guía de controles **ISO 27002:2013**. Dominio **A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**. Objetivo de control **A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO**. Control **A.6.2.1 Política de dispositivos móviles**: con la finalidad de implementar políticas de Seguridad de la Información que se constituyan en medidas concretas que mitiguen los riesgos de la seguridad de la información en el uso de dispositivos móviles en una organización

5. GLOSARIO

Confidencialidad: Pilar de seguridad de la información orientado al propósito de contar con procesos de lectura de información sólo al alcance de quienes deben tener autorización de acceso a los mismos.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato personal semiprivado: Son datos que no tienen una naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular, sino a un grupo de personas o a la sociedad en general. Para su tratamiento se requiere la autorización expresa del titular de la información (ejemplo: dato financiero y/o crediticio).

Datos sensibles: Son aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Disponibilidad: Requerimiento a los sistemas de información para que siempre estén prestos a ser usados; sin embargo, por la naturaleza de los componentes electrónicos que los conforman, nunca habrá disponibilidad total.

Dispositivo móvil: Elemento electrónico de tamaño pequeño, con capacidades de procesamiento de datos, conexión a Internet y memoria; son ejemplos de estos: celulares inteligentes, tabletas y portátiles.

Información: Conjunto de datos que organizados en determinado contexto tienen significado o importancia.

Información pública: Es aquella en poder de los sujetos obligados, contenida en documentos, archivos, datos, bases de datos, comunicaciones y todo tipo de registros que documenten el ejercicio de sus facultades o actividades, que consten en cualquier medio, ya sea impreso, óptico o electrónico, independientemente de su fuente, fecha de elaboración, y que no sea confidencial o reservada. Dentro de la información pública se encuentra un subconjunto de información denominado "información oficiosa", la cual debe de ser publicada de forma inmediata sin que ninguna persona lo solicite. Esta información puede estar impresa o colgada en los sitios web de las instituciones y deben entregártela en el mismo momento en que lo solicites.

Información reservada: Es la información pública cuyo acceso se restringe de manera expresa, debido a un interés general durante un periodo determinado y por causas justificadas. Por ejemplo, los planes militares secretos, las negociaciones internacionales o cualquier tipo de negociación o discusión que se tenga, mientras no se adopte una decisión definitiva. O toda aquella información que esté relacionada con la investigación o persecución de actos ilícitos o que genere una ventaja indebida en perjuicio de un tercero.

Información confidencial: Es la información privada en poder de los sujetos obligados, cuyo acceso público se prohíbe por mandato constitucional o legal en razón de un interés personal jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituiría una invasión a la privacidad de la persona. A esta información solo tendrán acceso las personas que son dueñas de ella. Dentro de la información confidencial están los datos personales la cual es la información privada de una persona, como por ejemplo su nacionalidad, domicilio, patrimonio, dirección electrónica, número de teléfono o cualquier otra parecida.

Ingeniería social: Práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Asimismo, técnica utilizada para obtener datos, acceso o privilegios a sistemas de información o dispositivos, de tal modo que permite la ejecución de acciones maliciosas para comprometer información e infraestructura tecnológica de una organización.

Integridad: Pilar de seguridad de la información, desde donde se orienta el propósito de tener procesos de escritura de información solo al alcance de quienes deben tener autorización a éstos.

SGSI: Subsistema de Gestión de Seguridad de la Información.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

URL (acrónimo de Uniform Resource Locator): Secuencia de caracteres utilizada para nombrar recursos en internet para su localización o identificación.

6. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

- El propósito de las redes institucionales es facilitar las labores propias de todas y cada una de las personas autorizadas al acceso de estas, sean servidores públicos, contratistas y/o colaboradores, en adelante los usuarios.

- Los registros de actividades en las redes institucionales están sujetos a ser monitoreados, auditados y accesibles en los casos permitidos por la Ley.

- El servicio de conectividad asignado a los usuarios debe ser utilizado para la atención de sus requerimientos y necesidades propias en el ejercicio de sus funciones.

- La SED definirá los lineamientos para la conectividad en las redes institucionales, mediante dispositivos móviles (obligaciones y prohibiciones) que deben cumplir todos los usuarios.

- La SED se reserva el derecho a permitir o bloquear el acceso de conectividad a sus redes institucionales, en las cuales se evidencie un uso inadecuado o que infieran en el incumplimiento de las políticas establecidas en el presente documento.

- La SED debe establecer procedimientos e implantar controles que permitan detectar intentos de acceso malintencionados externos a través de las redes institucionales, así como la de proteger la información que se encuentren en las aplicaciones accesibles a través de estas redes.

7. LINEAMIENTOS PARA EL USO DE DISPOSITIVOS MOVILES Y REDES INSTITUCIONALES

7.1 LINEAMIENTOS DE SEGURIDAD PARA EL USO DE DISPOSITIVOS MÓVILES QUE ACCEDAN A LA INFORMACIÓN DE LA SED A TRAVÉS DE SUS REDES INSTITUCIONALES.

7.1.1 Para niveles Central y Local

Los usuarios que hagan uso de dispositivos móviles para almacenar o acceder a la información de la SED a través de estos dispositivos como teléfonos inteligentes (Smartphones), Tabletas (tablets) u otros dispositivos corporativos electrónicos, deberá:

- Diligenciar la solicitud a la Oficina Administrativa de RedP (OAREDP) a través del aplicativo que se disponga para la habilitación de dispositivos móviles, con el propósito de que la OAREDP asigne (o rechace) a la red correspondiente, de acuerdo con la necesidad de trabajo requerida por el solicitante, aceptando automáticamente el cumplimiento de la política de dispositivos móviles del presente documento.

- Aceptar las configuraciones de seguridad, en caso de que estas se requieran, que se aplicarán en el dispositivo móvil, las mismas no podrán modificarse mientras se acceda o almacene información de la SED.

- Se prohíbe el uso de aplicaciones, o acceder a sitios web que atenten o saboteen la integridad, disponibilidad y confidencialidad de las redes institucionales de la SED y/o a la información almacenada en la Entidad.

- Se prohíbe la alteración de la información que identifica al dispositivo móvil (IMEI, Dirección MAC, etc.), luego de haber solicitado el acceso a las redes institucionales de la Entidad. En caso de que, por fuerza mayor, se hubiese realizado esta modificación al dispositivo, el usuario deberá hacer una nueva solicitud de acceso con la nueva información del dispositivo móvil.

- Se prohíbe compartir la configuración y/o contraseñas de dispositivos móviles para acceder a las redes institucionales de la SED, con los demás usuarios, funcionarios y/o terceros.

Únicamente el personal autorizado de Soporte SED está autorizado a instalar las configuraciones necesarias en cada dispositivo móvil.

- En caso de pérdida o hurto del dispositivo móvil, el usuario deberá reportar la novedad ante la mesa de soluciones TIC en el correo soportesed@educacionbogota.edu.co, considerando que cada usuario será responsable de las actividades realizadas a través del dispositivo.

- La SED recomienda:

  I. Instalar y configurar un software de antivirus en cada dispositivo móvil a los que accederá el usuario.

  II. Establecer un mecanismo de control de acceso al dispositivo móvil, como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital. No se recomienda el mecanismo de reconocimiento facial, debido a que algunos dispositivos presentan fallas de seguridad mediante dicho mecanismo.

  III. Configurar el bloqueo de pantalla para un máximo de 2 minutos de inactividad.

  IV. Activar cifrado del dispositivo móvil.

- Los dispositivos móviles corporativos no se deben conectar a computadores públicos o a redes Wifi públicas. (por ejemplo, aquellas que se pueden encontrar en hoteles, cafés internet, entre otros).

- Es prohibido almacenar videos, fotografías o información personal en los dispositivos asignados, dichos dispositivos son para uso exclusivo de actividades laborales.

- Cuando se trate de dispositivos móviles personales, el soporte técnico únicamente cumplirá con la función de brindar la conectividad de red a estos dispositivos, más no estarán disponibles para realizar soporte técnico y/o ningún tipo de mantenimiento.

- Se autoriza el uso de WhatsApp para efectos de comunicación, más no para el envío de información sensible o confidencial, de videos, documentos, fotografías, entre otros. La herramienta en mención no cuenta con soporte técnico por parte de la Mesa de Servicios de la Entidad y su uso es netamente responsabilidad del usuario.

NOTA: La herramienta corporativa de la entidad es Microsoft Teams.

7.1.2 Para Nivel Institucional

La conectividad de dispositivos móviles será exclusivamente para aquellos que pertenezcan al inventario de la Secretaría de Educación del Distrito, sin excepción alguna. El soporte técnico únicamente estará disponible para dar conectividad de red a los dispositivos móviles en mención.

7.2 LINEAMIENTOS DE SEGURIDAD PARA EL PERSONAL TÉCNICO ENCARGADO DE CONFIGURAR LOS DISPOSITIVOS MÓVILES (SOPORTE SED).

Es de vital importancia, que el personal técnico encargado de configurar los dispositivos móviles, acate las siguientes directrices para el cumplimiento de la política:

- Hacer el registro de la información que identifica a los dispositivos móviles (Direcciones MAC), que accederán a las redes institucionales de la SED.

- Llevar un registro de las actividades realizadas por cada dispositivo móvil conectado a las redes institucionales de la SED.

- Aplicar las configuraciones necesarias para que los dispositivos móviles puedan acceder a los aplicativos, sitios web y/o plataformas de la SED según requerimientos necesarios.

- Aplicar las restricciones necesarias desde los servidores, para impedir el acceso a sitios no deseados o descarga de aplicativos que distraigan, obstruyan o no aporten a la productividad de la SED.

- Según sea requerido, monitorear las actividades de cualquier dispositivo móvil conectado a las redes institucionales.

- Bloquear e impedir el acceso a las redes institucionales a aquellos dispositivos móviles que incumplan con la política del presente documento.

7.3 AUDITORÍA Y REVISIÓN DE LA POLÍTICA DE USO DE DISPOSITIVOS MÓVILES EN LAS REDES INSTITUCIONALES DE LA SED.

En cualquier momento, el Equipo de Seguridad Digital de la SED podrá verificar el cumplimiento de la política directamente en los dispositivos móviles que hagan parte del inventario de la SED.

Las Auditorías Internas o por parte de terceros, pueden realizar la verificación de las configuraciones de los dispositivos móviles y su cumplimiento con los lineamientos de esta política.

8. PÉRDIDA DEL DISPOSITIVO

En caso de pérdida o hurto de dispositivos móviles que se conecten o almacenen información de la Secretaría de Educación del Distrito, se debe reportar la perdida a la Oficina de las TIC lo más pronto posible, esto se puede informar a la mesa de soluciones al correo soportesed@educacionbogota.edu.co quienes informarán a los funcionarios encargados del inventario en la Entidad.

9. INCUMPLIMIENTO DE LA POLÍTICA

El uso inadecuado o el incumplimiento de la **política de uso de dispositivos móviles en las redes institucionales de la SED**, traerá consigo consecuencias administrativas, disciplinarias o legales, así como aquellas incluidas en la normativa del Gobierno Nacional y/o Territorial, relacionadas con la seguridad y la privacidad de la información.

10. RESPONSABILIDADES

- **Jefe de la Oficina OAREDP:** Designar el personal apto para que configure los dispositivos móviles, atendiendo los lineamientos de seguridad precisados en la política.

- **Equipo de Seguridad de la Información:** Velar por el desempeño y el cumplimiento de la presente política, certificando los niveles de seguridad proporcionados para el uso de los dispositivos móviles institucionales.

- **Personal Institucional:** Hacer uso responsable de los dispositivos móviles atendiendo los lineamientos concretados por la entidad.

Proyectó: Duber Jair Rocha Botero– Profesional Universitario OAREDP

Revisó: Equipo Seguridad Digital OAREDP

Aprobó: Equipo Técnico de Seguridad Digital – Marzo 2022