LINEAMIENTO PARA EL CONTROL DE USO DE APLICACIONES Y SOFTWARE NO AUTORIZADO, CONTROL 8.7 (Protección Contra Malware)

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

Versión 1.0
Febrero 2026

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

Tabla de Contenido

Índice de Tablas

VOCABULARIO

Autorización Segura: Principio de inclusión de software en la Lista Blanca solo después de una evaluación de riesgo C.I.D., que verifica que no permite la fuga de datos ni la elusión de controles.

C.I.D (Confidencialidad, Integridad y Disponibilidad): es el modelo fundamental de ciberseguridad que guía la protección de activos de la información con los criterios de seguridad:

- ✓ **Confidencialidad:** la información sea accesible únicamente por personas, procesos o sistemas debidamente autorizados.
- ✓ **Integridad:** la información mantenga su exactitud, completitud y consistencia, evitando alteraciones no autorizadas o accidentales.
- ✓ **Disponibilidad:** la información y los servicios asociados se encuentren accesibles y operativos cuando sean requeridos por los usuarios autorizados.

Elemento de Configuración (CI): Definición técnica en SCCM que especifica un requisito de cumplimiento, como la presencia de una aplicación o la versión mínima.

Elusión de Controles: Cualquier acción o software que desactive o evite las defensas de seguridad del sistema (ej. *firewall* local, antivirus, *agentes DLP*).

FOSS (Free and Open-Source Software): Se refiere a programas cuyo código fuente está disponible para que los usuarios lo utilicen, estudien, modifiquen y distribuyan libremente bajo los términos de una licencia específica.

Lista Blanca (Whitelist): El catálogo central de software que está permitido instalar

Lista Negra (Blacklist): Catálogo de software explícitamente prohibido debido a riesgos críticos (ej. KMSPico, software obsoleto)

Principio de Mínimo Privilegio (MMP): Política que limita a todos los usuarios (administrativos, docentes y estudiantes) a operar con permisos de Usuario Estándar, impidiendo la instalación de software no autorizado.

Software Restriction Policies (SRP): Capacidades nativas de Windows configuradas localmente para permitir o denegar la ejecución de aplicaciones por *hash* o ruta de archivo, utilizado en entornos sin GPOs o AppLocker centralizados.

Software Autorizado: Aplicación o programa aprobado e incluido en la Lista Blanca, cuya instalación y versión es verificada y gestionada activamente.

Software No Autorizado: Cualquier aplicación no incluida en la Lista Blanca, o aquellas categorizadas en la Lista Negra

SCCM: Microsoft Configuration Manager. Herramienta propietaria utilizada para la gestión de activos, el cumplimiento de políticas, el inventario y la remediación de software.

SAM (Software Asset Managemen): Es el proceso de gestionar y optimizar la compra, uso y desmantelamiento del software en una organización para controlar costos, mitigar riesgos y maximizar el valor de las inversiones en licencias.

Intune: Solución de administración de puntos finales (UEM) basada en la nube que unifica la seguridad, el acceso y la gestión de dispositivos (MDM) y aplicaciones (MAM)

ACL: Listas de Control de Acceso mediante Directorio Activo

1 JUSTIFICACIÓN

El uso de software no autorizado, inseguro, obsoleto o sin licenciamiento válido representa un riesgo directo para la seguridad de la información, al comprometer los criterios de Confidencialidad, Integridad y Disponibilidad (C.I.D.). Este tipo de prácticas incrementa la exposición a incidentes de seguridad, tales como accesos no autorizados, alteración o pérdida de información, indisponibilidad de los servicios tecnológicos y propagación de malware, con impacto sobre la continuidad operativa y el cumplimiento de los objetivos institucionales.

Dada la realidad operativa de la Secretaría de Educación del Distrito, donde el Nivel Central cuenta con gestión centralizada mediante SCCM o Intune, pero los Niveles Local e Institucional carecen de herramientas de administración centralizada de *endpoints* (sin SCCM, AD o LDAP), este lineamiento es fundamental para:

En atención a la realidad operativa de la Secretaría de Educación del Distrito (SED), se reconoce que el Nivel Central cuenta con esquemas de gestión centralizada de equipos mediante herramientas como SCCM o Intune, mientras que los Niveles Local e Institucional no disponen de plataformas de administración centralizada de endpoints (como SCCM, Active Directory o LDAP). En este contexto, el presente lineamiento resulta fundamental para:

1. Establecer controles obligatorios basados en políticas y configuración local para los Niveles Local e Institucional, asegurando el cumplimiento de ISO 27001:2022 a pesar de la ausencia de herramientas de gestión remota.

2. Garantizar la Autorización y uso seguro de software (incluido el educativo), asegurando que cumpla con confidencialidad, integridad y disponibilidad (C.I.D.), previniendo la fuga de datos personales y corporativos y la elusión de controles en todos los niveles.
3. Proveer un marco de control coherente y diferenciado, que reconozca las necesidades administrativas e institucionales del Nivel Central y Local, así como las particularidades operativas y pedagógicas del Nivel Institucional, sin menoscabar los principios de seguridad de la información.

2 OBJETIVOS

El lineamiento tiene como objetivos principales:

1. Garantizar la Seguridad (C.I.D.): Asegurar que todo software autorizado para su instalación y uso mantenga los principios de Confidencialidad, Integridad y Disponibilidad de la información.

2. Control de Riesgo Cero Tolerancia: Prevenir que la permisividad en el software

educativo (Nivel Institucional) pueda ser utilizada para eludir los controles de seguridad (ej. sandboxing, firewalls) o causar la fuga de datos personales y sensibles.

3. Control Diferenciado: Implementar políticas de Lista Blanca y Lista Negra y mecanismos de control específicos para los tres niveles, priorizando el Principio de Mínimo Privilegio (MMP) como control fundamental en entornos no gestionados.

4. Cumplimiento Normativo: Satisfacer los requisitos del control A.8.7 Protección Contra Malware de la ISO 27001:2022.

3 ALCANCE

Este lineamiento aplica a todos los activos de información y sistemas informáticos propiedad de la Secretaría de Educación del Distrito de Bogotá. El presente lineamiento aplica a todos los activos de información y sistemas informáticos de propiedad, custodia o administración de la Secretaría de Educación del Distrito de Bogotá, independientemente de su ubicación, nivel operativo (Nivel Central, Nivel Local o Nivel Institucional) o modalidad de uso.

Comprende, entre otros, equipos de cómputo, dispositivos móviles, servidores, sistemas de información, aplicaciones, software educativo y administrativo, medios de almacenamiento y recursos tecnológicos, utilizados por funcionarios, contratistas, docentes, directivos, estudiantes o terceros autorizados, en el marco del cumplimiento de las funciones institucionales.

El control se implementará mediante mecanismos específicos basados en la capacidad de gestión de cada nivel:

Tabla 1 Capacidad de Gestión por Nivel

Nivel Institucional	Gestión de Máquinas	Mecanismo de Control Principal	Foco en el Control
1. Nivel Central	Centralizada (SCCM - Intune)	SCCM, Intune, Inventario automatizado, Desinstalación forzosa.	Confidencialidad (Datos Corporativos).
2. Nivel Local	Sin Gestión Centralizada	Políticas Locales (MMP), Scripts de Auditoría Manual.	Integridad (Cumplimiento de Políticas).
3. Nivel Institucional	Sin Gestión Centralizada	Políticas Locales (MMP), Software Restriction Policies (SRP), Auditoría Manual.	Disponibilidad y Uso Educativo Seguro.

El lineamiento es de aplicación obligatoria para todos los funcionarios, contratistas, proveedores y cualquier usuario con acceso a los activos de información administrados.

4 ROLES Y RESPONSABILIDADES

La responsabilidad de la implementación y el mantenimiento del control “A.8.7 Protección Contra Malware” se asigna formalmente de la siguiente manera:

Tabla 2 Roles y Responsabilidades

Nivel	Rol Principal	Responsabilidades Específicas del Control 8.7 Protección Contra Malware
Liderazgo / Gobierno	Oficial de Seguridad de la Información / Oficial de Seguridad Informática	Aprobación y Gobernanza: • Aprueba: formalmente las Listas Blanca y Negra. • Autoriza: el uso de SCCM o Intune como herramienta primaria de control 8.7. • Evalúa: el reporte trimestral de cumplimiento del control.
Técnica / TI Operaciones	Líder TI y Administrador de SCCM * Intune	Implementación y Mantenimiento: • Mantiene: operativa la infraestructura de SCCM - Intune. • Crea: los Despliegues Requeridos y las Bases de Configuración de cumplimiento (CIs) para hacer cumplir las Listas Blanca y Negra. • Mínimo Privilegio: mediante GPOs, ACLs SCCM, Intune.
Ciberseguridad	Equipo de Estrategia y Gobierno	Definición y Detección: • Define: los criterios de riesgo para la inclusión de software en las listas. • Analiza: los reportes de incumplimiento de SCCM – Intune e identifica incidentes de software no autorizado. • Investiga: la causa raíz de las instalaciones no autorizadas.
Operativa/Ejecución	Gestión de Activos (SAM)	Licenciamiento: Verifica: y mantiene la trazabilidad de las licencias de todo el software Comercial/Licenciado que se incluye en la Lista Blanca.

Nivel	Rol Principal	Responsabilidades Específicas del Control 8.7 Protección Contra Malware
Operativa/Ejecución	Mesa de Servicio	1. Recibir, registrar y clasificar todas las solicitudes relacionadas con instalación, actualización, desinstalación o modificación de software en los equipos institucionales. 2. Verificar que la solicitud se encuentre debidamente justificada y alineada con las funciones del solicitante. 3. Validar que el software requerido cumpla con los lineamientos de licenciamiento, seguridad de la información y compatibilidad tecnológica definidos por la Entidad. 4. Escalar al área técnica correspondiente para su análisis, aprobación o ejecución cuando aplique. 5. Mantener trazabilidad completa del requerimiento, incluyendo aprobación, instalación y cierre del caso. 6. Garantizar que no se ejecuten instalaciones de software sin el registro y autorización previa en la herramienta oficial de gestión de servicios.
Operativa/Ejecución	Usuarios Finales	Cumplimiento: Se abstiene: de intentar instalar cualquier software para el cual no tenga autorización explícita y que no esté disponible en el *Software Center* de SCCM - Intune.

5 LINEAMIENTO DE CONTROL Y APLICACIÓN

La Secretaría de Educación del Distrito establecerá y aplicará controles técnicos, administrativos y operativos orientados a prevenir, detectar y mitigar el uso de software no autorizado, inseguro, obsoleto o sin licenciamiento válido, con el fin de proteger los criterios de Confidencialidad, Integridad y Disponibilidad (C.I.D.) de la información.

Estos controles deberán implementarse de manera proporcional al nivel de riesgo, considerando la criticidad del activo de información, el nivel operativo (Nivel Central, Local e Institucional) y la disponibilidad de herramientas de administración tecnológica, y serán de obligatorio cumplimiento para todos los usuarios y terceros autorizados que utilicen los recursos tecnológicos de la entidad.

5.1 Autorización Segura (Aplicable a Todo Nivel)

Toda solicitud de software (libre, licenciado o educativo) debe pasar por la validación del Equipo de Estrategia y Gobierno antes de su inclusión en la Lista Blanca:

i. Garantía C.I.D.: El software debe ser la versión más reciente y estable. Se prohíbe el software obsoleto de la Lista Negra (ej. Apache Tomcat 7.0, GlassFish 4.1.1).

ii. Garantía Anti-Fuga de Datos (Confidencialidad): Se prohíbe el software que:
    1. Acceda o transmita datos personales o corporativos fuera de los canales aprobados.
    2. Requiera privilegios de acceso a la red o al sistema que excedan su función.
    3. Se utiliza una revisión estricta para software educativo que pueda acceder a datos de estudiantes o docentes.

iii. Garantía Anti-Elusión (Integridad): El software no debe requerir o permitir la desactivación de controles esenciales de seguridad del sistema operativo o del *endpoint*.

5.2 Implementación del Control por Nivel (Mecanismos sin Gestión Centralizada)

El Principio de Mínimo Privilegio (MMP) es el control de prevención fundamental para los Niveles Local e Institucional.

Nivel	**Mecanismo de Prevención Clave**	**Mecanismo de Detección Clave**	**Mecanismo de Remediación**
1. Central (Gestionado)	SCCM - Intune: Control del MMP, AppLocker, Despliegue de software solo por *Software Center*.	SCCM: Inventario de software automatizado y continuo (7 días).	SCCM: Despliegue Requerido de Desinstalación forzosa.

Nivel	Mecanismo de Prevención Clave	Mecanismo de Detección Clave	Mecanismo de Remediación
2. Local (No Gestionado)	MMP (Configuración Inicial): El equipo de TI Local debe asegurar que todas las cuentas de usuario adulto sean Usuarios Estándar en la imagen base del equipo.	Scripts de Auditoría Locales: El equipo de TI Local debe ejecutar quincenalmente scripts (PowerShell/Python/Bash) que extraigan el listado de software (Get-WmiObject -Class Win32_Product o registro) y lo comparen con las Listas Blanca/Negra.	TI Local: Desinstalación manual in situ del software de la Lista Negra y no autorizado.
3. Institucional (No Gestionado)	MMP y SRP (Configuración Inicial): MMP aplicado rigurosamente. SRP se configura localmente para bloquear la ejecución de cualquier aplicación en rutas de usuario temporal y carpetas *peer-to-peer*.	Scripts de Auditoría Locales: Ejecución quincenal por el equipo de TI designado. El foco es la detección de software de alto riesgo (Blacklist) y herramientas que comprometen la Integridad/Disponibilidad.	TI Local Designado: Desinstalación manual y bloqueo del equipo hasta la remediación.

5.3 Controles de Detección y Remediación (SCCM - Intune)

i. Inventario y Detección Continua: SCCM - Intune debe configurarse para ejecutar un Inventario de Software completo en todos los *endpoints* gestionados con una frecuencia mínima de cada 7 días.

ii. Monitorización de Cumplimiento (*Whitelist*): El Administrador de SCCM - Intune implementará Bases de Configuración con Elementos de Configuración (CIs) que definan la presencia y versión del software autorizado. Los *endpoints* que reporten software desactualizado o faltante serán marcados como incumplimiento.

iii. Remediación Automatizada (*Blacklist*):
   - Todo software de la Lista Negra (ej. KMSPico, Java 1.4.1_01, GlassFish 4.1.1) debe configurarse en SCCM – Intune como un Despliegue Requerido de Desinstalación (Required Deployment - Uninstall).
   - SCCM - Intune debe garantizar que estas aplicaciones se eliminen de los *endpoints* automáticamente en cuanto se detecte su presencia.

iv. Generación de Alertas: Gobierno y Seguridad Digital utiliza los Reportes de Cumplimiento de SCCM para monitorear el estado de las Bases de Configuración de la Lista Negra. La detección de cualquier incumplimiento (software prohibido presente) debe generar una alerta de seguridad de prioridad Alta.

v. Control de detección y mitigación de software malicioso o no autorizado: Con el fin de mitigar los riesgos asociados a la permanencia de aplicaciones no autorizadas, software potencialmente malicioso o componentes residuales derivados de procesos de instalación o desinstalación incompletos, la entidad implementará como medida de control técnico el uso obligatorio de la solución Seguridad de Windows (Microsoft Defender Antivirus y/o Microsoft Defender for Endpoint) en todos los equipos administrados.

   Esta herramienta deberá mantenerse habilitada y configurada con las siguientes capacidades mínimas:

   - Protección en tiempo real, para la detección y bloqueo automático de malware, riskware, aplicaciones potencialmente no deseadas (PUA/PUP) y software no autorizado.
   - Actualización automática de firmas y motor de análisis, garantizando la detección de amenazas emergentes.
   - Análisis programados periódicos, configurados de manera centralizada.
   - Protección contra manipulación (Tamper Protection) habilitada para evitar la desactivación no autorizada del servicio.
   - Monitoreo y registro de eventos de seguridad, integrados al sistema de gestión centralizada.

   En caso de detección de software malicioso, no autorizado o potencialmente riesgoso, el sistema deberá ejecutar acciones automáticas de contención, cuarentena o eliminación conforme a las políticas definidas por la Entidad.
   Este control actúa como mecanismo preventivo y detectivo complementario a las herramientas de gestión de configuración y despliegue de software, fortaleciendo el cumplimiento de los principios de integridad, disponibilidad y seguridad de la información.

6 CANAL OBLIGATORIO PARA SOLICITUDES

Toda solicitud de instalación, actualización, modificación o desinstalación de software deberá ingresar obligatoriamente a través de la herramienta oficial de Mesa de Servicio dispuesta por la Entidad.

No se atenderán solicitudes realizadas por canales informales tales como correos

electrónicos directos, mensajes instantáneos, llamadas telefónicas sin registro o solicitudes verbales. La ausencia de registro formal impedirá la ejecución del requerimiento.

Este mecanismo garantiza:

- Trazabilidad.
- Control de cambios.
- Validación de seguridad.
- Cumplimiento de políticas institucionales.
- Evidencia para auditoría.

Aprobado por: MILENA DEL PILAR SANDOVAL GOMEZ
Jefe Oficina de Tecnologías de la Información y las Comunicaciones - OTIC

Elaborado: Juan Carlos Parra Moreno
Oficial Seguridad Informática - OTIC

Revisado: Henry Alexander Moyan
Oficial Seguridad de la Información – OTIC

Alicia Aidée Castro López
Gestor de Activos TI – OTIC

Revisado: Jairo Alberto Orduz Salamanca
Gestor de Activos TI – OTIC

José Daniel Mahecha
Gestor de Activos TI – OTIC

Revisado: Jasson Smith Castro L.
Profesional Especializado – OTIC

Camilo Arturo Sierra Suárez
Contratista – OTIC