MANUAL DE USO DE SALAS DE INFORMÁTICA - IED

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

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

Versión 1.0
Noviembre 2025

Tabla de Contenido

1 Introducción 4
2 Objetivos 4
3 Alcance 5
4 Controles y Buenas Prácticas 5
4.1 Seguridad Física y Control de Acceso 5
4.2 Ubicación y Protección de Equipos 6
4.3 Gestión de Estaciones de Trabajo 7
4.4 Gestión de Software y Cambios 8
4.5 Seguridad Lógica y Navegación 9
4.6 Gestión de Incidentes y Responsabilidades 10
4.7 Mantenimiento y Limpieza de Equipos 11
4.8 Disposición Final de Equipos 11
4.9 Señalización Visible 12
4.10 Apertura y Cierre de la Sala 12
5 Responsabilidades del Usuario 13

VOCABULARIO

Activos de Información: Elementos que contienen o manipulan información, tales como archivos, bases de datos, contratos, resoluciones, manuales, aplicaciones, software, equipos informáticos, equipos de comunicaciones, redes y talento humano.

Antivirus: Herramienta de software diseñada para proteger los sistemas operativos y equipos contra actividades maliciosas, como virus, gusanos, troyanos y otras formas de malware.

Confidencialidad: principio de seguridad de la información que garantiza que los datos sean accesibles únicamente para aquellas personas autorizadas para su consulta o procesamiento.

Disponibilidad: Principio de seguridad de la información que asegura que los sistemas y datos estén accesibles y operativos cuando sean requeridos por los usuarios autorizados.

Grooming: Conducta en la que un adulto se gana la confianza de un menor de edad a través de internet con fines de abuso sexual.

Hardware: Componentes físicos que conforman un sistema informático, incluyendo computadores, monitores, teclados, mouse, impresoras, dispositivos de red, entre otros.

IED (Institución Educativa Distrital): Establecimiento educativo oficial perteneciente al sistema educativo de la ciudad de Bogotá, administrado por la Secretaría de Educación del Distrito.

Incidente de Seguridad: Evento adverso o no deseado que afecta o puede afectar la confidencialidad, integridad o disponibilidad de los activos de información.

Integridad: principio de seguridad de la información que garantiza que los datos no sean modificados o alterados de manera no autorizada, manteniendo su exactitud y completitud.

ISP (Proveedor de Servicios de Internet): Empresa externa que proporciona acceso a internet y, en algunos casos, otros servicios TIC como hospedaje de sitios web.

Malware: Programa o código malicioso diseñado para infiltrarse, dañar o comprometer sistemas informáticos sin el consentimiento del usuario. Incluye virus, gusanos, troyanos, ransomware, spyware, entre otros.

Mesa de Servicios TIC: Unidad funcional encargada de recibir, gestionar y dar respuesta a los incidentes y requerimientos relacionados con los servicios de

Tecnologías de la Información y las Comunicaciones de la SED.

Microsoft 365: Conjunto de aplicaciones y servicios en la nube licenciados por la Secretaría de Educación del Distrito (SED) que incluye, entre otros, OneDrive (almacenamiento en la nube) y SharePoint (colaboración y gestión documental), constituyendo la plataforma institucional autorizada para el resguardo de información en el entorno educativo.

QoS (Calidad de Servicio): Conjunto de tecnologías y mecanismos que permiten gestionar el tráfico de red para priorizar ciertos tipos de datos, garantizando un rendimiento adecuado para servicios críticos, como los de impacto pedagógico.

Rack: Estructura metálica estandarizada diseñada para albergar, organizar y proteger equipos tecnológicos como servidores, switches, routers y unidades de almacenamiento.

Sexting: Práctica de enviar o compartir imágenes, videos o mensajes de contenido sexual explícito a través de dispositivos electrónicos y plataformas digitales.

Sistema de Alimentación Ininterrumpida (UPS): Dispositivo eléctrico que proporciona energía de respaldo a los equipos conectados en caso de cortes o fluctuaciones de voltaje, protegiéndolos de daños y permitiendo el apagado seguro.

Software: Conjunto de programas, aplicaciones y sistemas operativos que permiten el funcionamiento de los equipos informáticos y la ejecución de tareas específicas.

TIC (Tecnologías de la Información y las Comunicaciones): Conjunto de tecnologías desarrolladas para gestionar, almacenar, procesar y transmitir información de un lugar a otro, incluyendo hardware, software, redes y servicios asociados.

Trashing: Práctica de obtener información confidencial o sensible a través de la revisión de residuos, basura electrónica o documentos desechados.

VPN (Red Privada Virtual): Conexión segura que permite a los usuarios acceder a una red privada a través de internet, cifrando la comunicación y ocultando la dirección IP real del usuario.

1 INTRODUCCIÓN

Las Salas de Informática de las Instituciones Educativas Distritales (IED) son espacios fundamentales para el desarrollo de competencias digitales, el acceso a la información y el fortalecimiento de los procesos de enseñanza-aprendizaje. Estos entornos albergan recursos tecnológicos que representan una inversión significativa para la entidad y constituyen herramientas esenciales para la formación de los estudiantes en la era digital.

El uso adecuado de estos espacios y equipos no solo garantiza su disponibilidad y durabilidad, sino que también protege la integridad de los datos, la privacidad de los usuarios y la continuidad de las actividades académicas. El desconocimiento o la aplicación inadecuada de las normas de uso puede derivar en daños físicos, afectaciones a la infraestructura de red, pérdida de información o incidentes de ciberseguridad que impacten a toda la comunidad educativa.

El presente Manual de Uso de Salas de Informática se constituye como un instrumento práctico y pedagógico dirigido a toda la comunidad educativa (estudiantes, docentes, directivos y personal administrativo), con el propósito de establecer pautas claras para el comportamiento seguro, responsable y eficiente dentro de estos espacios.

Este manual se fundamenta en los principios de seguridad de la información establecidos por la norma ISO/IEC 27001:2022 y se alinea con las políticas y lineamientos TIC vigentes en la Secretaría de Educación del Distrito, garantizando la protección de los activos de información y la continuidad del servicio educativo. De manera complementaria, el presente manual se expide en cumplimiento de la Ley 2489 de 2025, cuyo objeto es promover, proteger y garantizar entornos digitales sanos y seguros para la niñez y adolescencia, así como del Decreto 0385 de 2026 que la reglamenta. En este marco, las Salas de Informática de las IED se constituyen como entornos protectores de aprendizaje donde se implementan, desde el diseño de los servicios, medidas que priorizan la seguridad y privacidad de los menores de edad.

2 OBJETIVOS

Establecer las directrices, controles y buenas prácticas para el uso adecuado, seguro y eficiente de las Salas de Informática en las Instituciones Educativas Distritales, con el fin de:

- Garantizar la disponibilidad, integridad y confidencialidad de los recursos tecnológicos (hardware, software y conectividad).
- Proteger la infraestructura física y lógica de las salas de informática frente a daños, accesos no autorizados e incidentes de seguridad.
- Promover una cultura de uso responsable y cuidado de los bienes institucionales entre los estudiantes, docentes y personal administrativo.
- Asegurar el cumplimiento de los controles establecidos en la norma ISO/IEC 27001:2022 para la gestión de activos, control de acceso físico y seguridad

de los equipos.
- Minimizar los riesgos asociados a la operación de los equipos y la navegación en internet, previniendo afectaciones a la red institucional y a la experiencia educativa de los usuarios.

Este manual actúa como el marco operativo para la ejecución segura de los proyectos PRY-25 (Estrategia de Uso y Apropiación de TI) y PRY-30 (Servicio de Conectividad SED) del PETI 2024-2027, promoviendo el desarrollo de competencias de ciudadanía digital, pensamiento computacional y uso ético de las tecnologías de la información en el aula.

3 ALCANCE

El presente manual aplica a todos los estudiantes, docentes, directivos docentes, contratistas, practicantes y personal administrativo que hagan uso de las Salas de Informática en las Instituciones Educativas Distritales (IED), así como a los equipos de cómputo, periféricos, dispositivos de red y demás elementos tecnológicos que conforman dichos espacios.

4 CONTROLES Y BUENAS PRÁCTICAS

4.1 Seguridad Física y Control de Acceso

(Alineado con controles ISO 27001:2022 - A.7.1, A.7.2, A.7.3, A.7.4)

Objetivo: Prevenir el acceso no autorizado, daños o interferencias a la infraestructura tecnológica.

- Acceso Restringido: La sala de informática permanecerá cerrada y solo será accesible durante los horarios establecidos por el docente o personal autorizado. El ingreso de los estudiantes se realizará **en grupo y bajo la supervisión directa del docente responsable**, quien velará por el control del acceso y el uso adecuado de los equipos.

  En caso de que un estudiante ingrese de manera individual (por ejemplo, para recuperación, consulta o trabajo extracurricular), deberá ser **registrado por el docente encargado** en el libro de control de acceso, consignando nombre completo, curso, hora de ingreso y salida, y actividad a realizar.
- Monitoreo y Protección de Equipos Críticos (A.7.4):
  Los equipos activos de red (rack, switch, router, UPS) deben estar protegidos contra accesos no autorizados mediante medidas físicas:
  - Gabinete o rack con cerradura.
  - Ubicación en zona de supervisión directa.
  - Prohibición de manipulación por parte de estudiantes.
  - Cualquier intervención técnica debe ser realizada exclusivamente por personal de la OTIC o contratistas autorizados, y debe quedar registrada.

- Perímetros de Seguridad (A.7.1): Los equipos activos de red (rack, switches, routers, UPS) deben ser considerados áreas restringidas independientemente de su ubicación física. Para garantizar su protección:
    - Si la IED cuenta con un cuarto de cableado, este debe permanecer cerrado con llave y el acceso debe estar limitado exclusivamente al personal autorizado por la OTIC o al docente técnico designado.
    - Si el rack se encuentra dentro de la sala de informática, deberá permanecer cerrado con llave y ubicarse en un lugar visible que permita la supervisión directa. Los estudiantes no podrán manipularlo ni acercarse a él sin autorización.
    - En todos los casos, solo el personal de la OTIC, contratistas autorizados podrán acceder a los equipos activos de red para realizar mantenimiento o intervenciones técnicas.
    - Cualquier acceso debe quedar registrado (fecha, hora, persona, motivo) en el libro de novedades o bitácora de la sala.
- Prohibición de Alimentos y Bebidas: No ingresar con alimentos o bebidas para evitar daños por derrames en los equipos (teclados, mouse, CPU) y mantener la higiene del espacio.
- Prohibición de rayar o dañar infraestructura: No rayar mesas, paredes, ni tratar con descuido sillas o mobiliario. Es responsabilidad del usuario cuidar los bienes institucionales.

4.2 Ubicación y Protección de Equipos

(Alineado con controles ISO 27001:2022 - A.7.8, A.7.11, A.7.12)

Objetivo: Reducir los riesgos de daño físico, robo o interrupción del servicio.

- Ubicación Segura: Las CPU deben estar ubicadas en lugares que permitan la ventilación adecuada y reduzcan el riesgo de daño accidental. No colocar objetos sobre las torres o unidades del sistema.

- Protección Eléctrica (A.7.11): La conexión eléctrica de los equipos debe realizarse de acuerdo con su tipo y las condiciones de infraestructura de la IED:

    - Equipos de escritorio (CPU, monitor, etc.): Deben conectarse exclusivamente a tomacorrientes de color naranja (red regulada), protegidos por el UPS, para evitar daños por fluctuaciones de voltaje o apagados súbitos.

    - Equipos portátiles, tabletas y todo en uno: Pueden conectarse a cualquier tomacorriente disponible (naranja o blanco), ya que cuentan con fuentes de alimentación externas (adaptadores) que regulan el voltaje de manera interna. Sin embargo, se recomienda priorizar el uso de tomas reguladas cuando sea posible.

    - La red normal (tomacorrientes blancos) está destinada para impresoras, neveras, ventiladores, cargadores de portátiles y otros

equipos de alto consumo que pueden generar picos de voltaje. No deben conectarse equipos de escritorio a estas tomas.

- Seguridad del Cableado (A.7.12): No manipular los cables de red, eléctricos o de datos. Reportar cualquier anomalía al docente o a la Mesa de Servicios para evitar cortes o daños en la conectividad.
- No mover periféricos: Mouse, teclado, parlantes y cámaras son asignados a un equipo específico para facilitar el inventario y el control de daños. No se deben intercambiar entre equipos.
- No forzar elementos: No forzar conectores, puertos USB, botones de encendido u otros componentes. Tratar los equipos con cuidado.

4.3 Gestión de Estaciones de Trabajo

(Alineado con controles ISO 27001:2022 - A.7.7, A.8.1, A.8.7)

Objetivo: Proteger la información en los dispositivos finales y mantener el orden en las áreas de trabajo.

- Verificación Inicial: Al ingresar a la sala, verificar el estado del equipo asignado y, en caso de encontrar alguna anomalía (daño físico, falla técnica, etc.), informar de inmediato al docente a cargo.
  La identificación y seguimiento de los equipos de cómputo y periféricos se realizan conforme a la Práctica 12-PD-030 (Gestión de Inventario TIC), que establece los controles de placas, seriales y demás elementos de inventario tecnológico de la SED.
- Política de Escritorio y Pantalla Limpia (A.7.7): Al finalizar la sesión, el usuario debe cerrar todas las aplicaciones, archivos y sesiones del navegador. Los equipos deben quedar apagados y el puesto de trabajo organizado y limpio.
- Protección de Equipos (A.8.1):
  - No modificar la configuración del sistema operativo, ni cambiar la resolución de pantalla, fondo de escritorio o configuraciones de red sin autorización.
  - Técnicamente, esta restricción se encuentra garantizada por el modelo de administración de equipos en las IED, donde los usuarios (estudiantes y docentes) operan con cuentas locales sin privilegios de administración. Solo la cuenta de administrador, utilizada por la Mesa de Servicios TIC para labores de soporte y mantenimiento, cuenta con los permisos necesarios para realizar cambios en la configuración del sistema operativo, resolución de pantalla, fondo de escritorio o configuraciones de red.
  - En caso de que un usuario requiera realizar algún cambio en la configuración del equipo por razones pedagógicas o técnicas debidamente justificadas, deberá solicitar el acompañamiento de la Mesa de Servicios TIC a través de los canales establecidos (correo: soportesed@educacionbogota.edu.co o teléfono: 3241000 Ext: 3333).
- Protección contra Malware (A.8.7):

- El uso de dispositivos de almacenamiento personal (USB, discos externos, tarjetas de memoria) está restringido y solo se permitirá de manera excepcional, previa autorización del docente y después de realizar un escaneo completo con el antivirus institucional.
- Se prioriza el uso de Microsoft 365 (OneDrive/SharePoint) como mecanismo estándar para el intercambio y almacenamiento de archivos, reduciendo significativamente el riesgo de introducción de malware a la red institucional.
- Está prohibido conectar dispositivos de almacenamiento personal (USB, discos externos) sin la autorización del docente o sin previo escaneo con el antivirus institucional, para evitar la propagación de virus o malware.

- Almacenamiento de Archivos:
  - El almacenamiento de archivos académicos deberá realizarse prioritariamente a través de Microsoft 365 (OneDrive / SharePoint), herramienta licenciada por la SED que garantiza copias de seguridad automáticas, acceso desde cualquier equipo y protección contra pérdida de información.
  - El uso de dispositivos de almacenamiento personal (USB, discos externos, tarjetas de memoria) se considera una medida excepcional y sujeta a las siguientes condiciones:
    - Debe ser previamente autorizado por el docente a cargo.
    - El dispositivo deberá ser escaneado con el antivirus institucional antes de su conexión al equipo.
    - Los archivos deberán ser copiados al equipo y retirados del dispositivo al finalizar la sesión.
    - No se permite la ejecución directa de programas o aplicaciones desde el dispositivo USB.
  - Guardar archivos únicamente en los directorios autorizados. No almacenar archivos personales en el disco duro del equipo, ya que serán depurados periódicamente.
  - La SED, a través de sus lineamientos de filtrado web, bloquea el acceso a servicios de almacenamiento en la nube no institucionales, por lo que el uso de Microsoft 365 constituye el mecanismo autorizado para el resguardo de información en el entorno educativo.
  - Responsabilidad del usuario: El usuario es el único responsable de la pérdida de archivos almacenados en los equipos de la sala. Se recomienda hacer copias de seguridad con frecuencia.

Nota para docentes: Se sugiere destinar los últimos 5 minutos de cada clase para que los estudiantes guarden sus archivos en sus dispositivos personales o en la nube.

4.4 Gestión de Software y Cambios

(Alineado con controles ISO 27001:2022 - A.8.9, A.8.19, A.8.32)

Objetivo: Asegurar que el software instalado sea el autorizado y que los cambios sean controlados.

- Restricción de Instalación: Dentro de las salas de informática existe una restricción para la instalación de aplicaciones a nivel de usuario. Solo el administrador del sistema puede instalar aplicaciones.
- Instalación y Cambios (A.8.19 / A.8.32): Ningún usuario (docente, estudiante o administrativo) podrá instalar, desinstalar o modificar software, navegadores, extensiones o aplicaciones en los equipos de la sala. Cualquier requerimiento de nuevo software debe ser solicitado formalmente a la Mesa de Servicios de la SED para su evaluación e instalación por personal autorizado.
- Configuración (A.8.9): Solo el personal de la OTIC está autorizado para realizar cambios en la configuración de los equipos, red o servicios.

4.5 Seguridad Lógica y Navegación

(Alineado con controles ISO 27001:2022 - A.8.3, A.8.16, A.8.23)

Objetivo: Controlar el acceso a la información, garantizar un entorno digital seguro para los menores de edad y monitorear el uso adecuado de los recursos de red, en el marco de la normatividad vigente.

- **Marco Normativo para Entornos Digitales Seguros:** De conformidad con la Ley 2489 de 2025 y el Decreto 0385 de 2026, las Salas de Informática de las IED se constituyen como entornos protectores de aprendizaje. El servicio de navegación a Internet estará restringido de manera estricta bajo el **"Perfil Colegios"** (alineado con el Control A.8.23 de ISO 27001:2022), aplicando filtros automatizados que bloqueen categorías de contenido inadecuado, violento o publicitario dirigido a menores de edad, asegurando el Interés Superior del Menor en el ecosistema digital.
- **Filtrado Web:** La navegación se rige por los Lineamientos de Filtrado Web de la SED, que para el "Perfil Colegios" establece el bloqueo de categorías como contenido adulto, juegos de azar, violencia explícita, drogas, redes sociales abiertas, chats públicos, streaming recreativo, VPN públicas y servicios de proxy, garantizando que los recursos tecnológicos se enfoquen en fines educativos.
- Restricción de Acceso (A.8.3): El acceso a internet y a los recursos de la sala es exclusivo para fines educativos y de formación, alineado con los Lineamientos de Filtrado Web[1] de la SED.
- Monitoreo de Actividades (A.8.16): El uso de la red y los accesos a sitios web son monitoreados por la OTIC para garantizar el uso adecuado de los recursos y detectar comportamientos anómalos.
- Filtrado Web (A.8.23): La navegación estará restringida por los Lineamientos de filtrado web de la SED, que bloquean el acceso a sitios de contenido para

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

adultos, violencia, juegos, apuestas, drogas, hacking y otros no permitidos.

- Cuentas Personales: No vincular cuentas de correo personales en los equipos de la sala. No enviar cadenas de correo ni correos masivos desde los equipos institucionales.
- Redes Sociales y Filtrado Web: El acceso a plataformas de redes sociales se encuentra restringido por los Lineamientos de filtrado web de la SED, los cuales bloquean esta categoría de sitios para garantizar el uso adecuado de los recursos de red y enfocarlos en fines educativos. No está permitido el uso de redes sociales desde los equipos de las salas de informática. Cualquier solicitud de excepción para fines académicos debidamente justificados debe ser gestionada a través de la Mesa de Servicios TIC de la SED
- Reporte de Inconsistencias en el Filtrado: Si un usuario identifica que un sitio web con contenido educativo legítimo está siendo bloqueado de manera incorrecta, deberá reportarlo al docente a cargo, quien elevará la solicitud de revisión a la Mesa de Servicios TIC de la SED, siguiendo los procedimientos establecidos.
- Conexiones No Autorizadas: No realizar conexiones VPN no autorizadas ni compartir la clave de la red WiFi de la institución.
- Herramientas de Hackeo: No utilizar herramientas de hackeo ni intentar obtener contraseñas de red.

4.6 Gestión de Incidentes y Responsabilidades

(Alineado con controles ISO 27001:2022 - A.5.24, A.5.25, A.5.26, A.6.8)

Objetivo: Establecer un proceso claro para reportar y responder ante incidentes de seguridad.

- Reporte de Incidentes (A.6.8): Cualquier anomalía, daño físico, falla técnica o incidente de seguridad (ej. intento de acceso no autorizado, malware, contenido inapropiado) debe ser reportado de inmediato al docente encargado o a la Mesa de Servicios TIC, siguiendo los canales establecidos por la SED (correo: soportesed@educacionbogota.edu.co o teléfono: 3241000 Ext: 3333, Web: https://mesadeserviciosredp.educacionbogota.edu.co:442/login).
  La gestión de incidentes de hardware en el puesto de trabajo se rige por la Práctica 12-PD-025 (Gestión de Incidentes de Hardware en el Puesto de Trabajo), la cual establece los procedimientos para la atención de fallas físicas en computadores, periféricos y demás equipos tecnológicos de la sala.

  Cuando a través de la supervisión docente o del monitoreo lógico de la OTIC se detecten incidentes que afecten la integridad de los menores (tales como ciberacoso, grooming o acceso a contenidos de explotación sexual), se suspenderá de inmediato el acceso del usuario y se activará la ruta de atención del Comité Escolar de Convivencia de la IED, en estricto cumplimiento de la Ley 2564 de 2026, la Ley 1620 de 2013 y la Política de Tratamiento de Datos Personales de la SED.

- Sustracción de Elementos: No sustraer ni llevarse elementos de la sala de informática. Esta acción será considerada falta grave y reportada a las autoridades competentes.
- Consecuencias (A.6.4): El incumplimiento de las normas del presente manual, o el uso indebido de los recursos, estará sujeto a las medidas disciplinarias contempladas en el Manual de Convivencia de la IED, el Código Único Disciplinario y demás normas aplicables de la SED.

4.7 Mantenimiento y Limpieza de Equipos

(Alineado con ISO 27001:2022 - A.7.12, A.7.14)

Objetivo: Garantizar la operatividad y prolongar la vida útil de los equipos mediante mantenimiento preventivo.

- La limpieza física de los equipos (CPU, monitor, teclado, mouse) será realizada periódicamente por parte del personal de Mesa de Servicios TIC, utilizando los insumos y técnicas adecuadas para evitar daños.
- El mantenimiento preventivo de los equipos de cómputo se rige por el Proceso 12-PD-032 (Procedimiento Modelo de Enfoque Mantenimiento Preventivo - Obligación Contractual Operación Mesa de Soluciones TIC). La solicitud de mantenimiento preventivo deberá realizarse a través de la Mesa de Soluciones TIC, agendando la visita técnica mediante el correo soportesed@educacionbogota.edu.co, incluyendo tipo y cantidad de equipos a intervenir, así como las fechas disponibles para el mantenimiento.
- La OTIC a través de la Mesa de Servicios coordinará con la IED la ejecución de los mantenimientos preventivos periódicos (al menos una vez al año) para garantizar el estado óptimo de los equipos.
- La operación de la Mesa de Soluciones TIC se desarrolla conforme a la Práctica 12-PD-035 (Práctica Gestión Mesa de Soluciones TIC), que define los procedimientos para la atención de requerimientos y la prestación del servicio de soporte técnico en las IED.

4.8 Disposición Final de Equipos

(Alineado con ISO 27001:2022 - A.8.10)

Objetivo: Asegurar la disposición segura de equipos al final de su vida útil.

- Cuando un equipo de cómputo o periférico sea declarado inservible por parte de la OTIC, debe ser retirado de la sala y almacenado en un lugar seguro hasta su disposición final.
- Antes de la disposición final, todos los dispositivos de almacenamiento (discos duros, SSD, etc.) deben ser sanitizados mediante borrado seguro o destrucción física, conforme a los procedimientos establecidos por la OTIC. Hasta que dicho procedimiento sea formalizado y aprobado, la sanitización

de los dispositivos se realizará bajo los lineamientos técnicos generales de buenas prácticas en seguridad de la información, priorizando la destrucción física controlada como método que garantiza la irrecuperabilidad de los datos.

- La disposición final de los equipos será gestionada y coordinada exclusivamente por la OTIC a través de la Mesa de Servicios TIC de la SED, con el apoyo de la Dirección de Dotaciones Escolares cuando se requiera. La IED no podrá disponer directamente de los residuos electrónicos, ni entregarlos a terceros no autorizados.
- El proceso de disposición final se adelantará en articulación con las entidades autorizadas por el Distrito para la gestión de RAEE, como la Unidad Administrativa Especial de Servicios Públicos (UAESP), la Secretaría Distrital de Ambiente (a través del programa ECOLLECTA) o Computadores para Educar (CPE), según los canales y procedimientos vigentes.
- La OTIC, a través de la Mesa de Servicios TIC, será la encargada de obtener y custodiar el certificado de disposición final, documento que acredita el manejo ambientalmente responsable de los residuos y que deberá ser anexado al expediente de bajas de la IED.
- El control de inventario para la identificación y baja de los equipos se realiza conforme a la Práctica 12-PD-030 (Gestión de Inventario TIC), que establece los procedimientos para el seguimiento de placas, seriales y la gestión de bajas de activos tecnológicos.

4.9 Señalización Visible

Las normas de uso de la sala de informática deben estar publicadas en un lugar visible dentro del espacio (cartelera, afiche o pantalla), de manera que todos los usuarios puedan consultarlas fácilmente.

4.10 Apertura y Cierre de la Sala

(Alineado con ISO 27001:2022 - A.7.3)

Objetivo: Garantizar que la sala sea abierta y cerrada de manera segura, previniendo accesos no autorizados.

- La sala de informática debe ser abierta únicamente por el docente encargado o personal autorizado.
- Al finalizar la jornada, se debe verificar que:
  - Todos los equipos están apagados correctamente.
  - Las ventanas y puertas estén cerradas y aseguradas.
  - No haya elementos olvidados dentro de la sala.
- La llave de la sala debe ser custodiada por el docente encargado o la coordinación académica, y no debe ser entregada a estudiantes.

5 RESPONSABILIDADES DEL USUARIO

Los usuarios de las Salas de Informática (estudiantes, docentes, directivos, administrativos, contratistas, practicantes) tienen las siguientes responsabilidades:

1. Uso Exclusivo: Utilizar los equipos y recursos única y exclusivamente para fines académicos y educativos, de acuerdo con los lineamientos de la SED.
2. Custodia y Cuidado: Ser responsable del cuidado del equipo y puesto de trabajo asignado durante su uso, así como del mobiliario y elementos de la sala.
3. Reporte Inmediato: Reportar cualquier novedad (daño físico, falla técnica, contenido inapropiado, incidente de seguridad) al docente o personal a cargo de la sala.
4. Identificación: Identificarse mediante el carné institucional cuando sea requerido para acceder a la sala de informática.
5. Copia de Seguridad: Realizar copia de seguridad de su información almacenada en el equipo. La institución no se hace responsable de la pérdida de información debido a fallas técnicas o daños en los equipos.
6. Mantener el orden: Mantener el orden y la disciplina dentro de las salas de informática, evitando el uso como espacio de conversatorio, juegos u otras actividades no académicas.

Aprobado por: MILENA DEL PILAR SANDOVAL GOMEZ
Jefe - OTIC

Elaborado: Juan Carlos Parra Moreno
Oficial Seguridad Informática - OTIC

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

Revisado: Jasson Smith Castro L.
Profesional Especializado – OTIC

Revisado: Luz Dary Vargas Suarez
Profesional Especializado – OTIC

Revisado: Alicia Aidee Castro López
Profesional Universitario – OTIC

Revisado: Stephany Grey Suarez Galvan
Contratis – OTIC