Política de Seguridad de Laboratorios de Informática

# 1. Introducción

La presente política establece las normas y procedimientos para garantizar la seguridad de la información y de los equipos tecnológicos en los laboratorios de informática de la institución educativa. Su aplicación busca proteger la confidencialidad, integridad y disponibilidad de los recursos informáticos.

# 2. Objetivos

• Garantizar la confidencialidad, integridad y disponibilidad de la información.  
• Proteger los recursos tecnológicos de la institución.  
• Establecer responsabilidades claras para docentes, alumnos y personal administrativo.

# 3. Qué se puede hacer

• Uso de los laboratorios para actividades académicas autorizadas.  
• Navegación en internet solo con fines educativos.  
• Uso de cuentas institucionales con credenciales asignadas.  
• Guardado de trabajos en servidores o nubes institucionales.

# 4. Qué no se puede hacer

• Instalar software sin autorización.  
• Conectar dispositivos externos sin análisis previo (pendrives, discos externos).  
• Compartir usuarios y contraseñas.  
• Acceder a sitios web no permitidos (apuestas, descargas ilegales).  
• Modificar configuraciones de los equipos.

# 5. Cómo se debe hacer en la operación normal

• Iniciar sesión con usuario institucional.  
• Guardar trabajos en carpetas autorizadas.  
• Cerrar sesión o apagar el equipo al finalizar.  
• Reportar incidentes al área de sistemas.  
• Usar internet y software de acuerdo con los fines académicos.

# 6. Análisis de Riesgos

|  |  |  |
| --- | --- | --- |
| Riesgo | Impacto | Probabilidad |
| Robo de equipos | Alto | Medio |
| Incendio o corte eléctrico | Alto | Bajo |
| Virus o malware | Alto | Alto |
| Acceso no autorizado | Alto | Medio |
| Uso indebido por parte de alumnos | Medio | Alto |

# 7. Plan de Contingencia

• Copias de seguridad semanales en servidores externos.  
• Respuesta ante incidentes de malware: aislamiento del equipo y reinstalación.  
• Protocolos ante corte eléctrico: uso de UPS y generadores.  
• Procedimientos de recuperación de datos y restauración desde copias de seguridad.  
• Comunicación inmediata a los responsables de seguridad ante cualquier incidente.

# 8. Responsabilidades

• Área de sistemas: implementación, control y monitoreo.  
• Docentes: supervisión del uso de los laboratorios.  
• Alumnos: cumplimiento estricto de la política.  
• Administración: asignar recursos y verificar el cumplimiento.