Uso de Antivirus y Sistemas de Detección de Intrusos
Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila
(CECyTE Coahuila)

1. Objetivo

Establecer lineamientos para el uso, actualización y administración de software antivirus y sistemas de detección de intrusos (IDS/IPS), con el fin de proteger la infraestructura tecnológica y la información institucional contra amenazas internas y externas.

2. Alcance

Este documento aplica a todos los equipos de cómputo, servidores, dispositivos móviles y redes de comunicación del CECyTE Coahuila, así como al personal administrativo, docente, estudiantes y terceros que hagan uso de ellos.

3. Principios

- **Prevención:** Evitar la instalación y propagación de software malicioso.
- **Detección:** Identificar intentos de acceso no autorizado o actividades sospechosas.
- **Respuesta:** Actuar oportunamente ante incidentes de seguridad informática.

4. Lineamientos Generales

4.1 Uso de Antivirus

- Todos los equipos institucionales deberán contar con software antivirus autorizado por el área de TI.
- El antivirus deberá mantenerse **actualizado diariamente** mediante conexión a servidores oficiales.
- Se realizarán **escaneos completos semanales** en equipos de cómputo y servidores.
- Los usuarios tienen prohibido desactivar o modificar la configuración del antivirus sin autorización.
- El área de TI será responsable de monitorear alertas y reportes generados por el antivirus.

4.2 Sistemas de Detección y Prevención de Intrusos (IDS/IPS)

- La red institucional contará con sistemas IDS/IPS para monitorear tráfico y detectar intentos de intrusión.
- Se configurarán reglas de seguridad para identificar patrones de ataque conocidos y actividades anómalas.
- Los registros generados por IDS/IPS deberán revisarse **diariamente** por el área de TI.
- Ante la detección de un intento de intrusión, se aplicarán medidas inmediatas de bloqueo y aislamiento.
- Se mantendrá un **registro de incidentes** con fecha, hora, descripción y acciones correctivas aplicadas.

4.3 Responsabilidades de los Usuarios

- No instalar software no autorizado que pueda comprometer la seguridad.
- Reportar inmediatamente cualquier comportamiento extraño en el equipo (lentitud, ventanas emergentes, accesos no reconocidos).
- Evitar el uso de dispositivos externos sin autorización (USB, discos duros, etc.).

4.4 Responsabilidades del Área de TI

- Implementar y administrar las soluciones antivirus e IDS/IPS.
- Monitorear continuamente alertas y registros de seguridad.
- Coordinar acciones de respuesta ante incidentes.
- Capacitar a usuarios en buenas prácticas de seguridad informática.

5. Procedimientos ante Incidentes

- **Detección:** Identificación de virus, malware o intento de intrusión.
- **Notificación:** Reporte inmediato al área de TI.
- **Contención:** Aislamiento del equipo o red afectada.
- **Erradicación:** Eliminación del software malicioso o bloqueo del ataque.
- **Recuperación:** Restauración de sistemas y datos respaldados.
- **Documentación:** Registro del incidente y medidas aplicadas.

6. Vigencia

Este documento entra en vigor el **04 de febrero de 2026** y será revisado anualmente o cuando existan cambios relevantes en la infraestructura tecnológica o normativa aplicable.

Última actualización: 04 de febrero de 2026