Lineamientos de Uso de Sistemas y Comunicaciones
Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila
(CECyTE Coahuila)

1. Objetivo

Regular el uso de los sistemas informáticos, redes de comunicación y recursos tecnológicos del CECyTE Coahuila, garantizando su disponibilidad, seguridad y correcto funcionamiento.

2. Alcance

Aplica a todo el personal administrativo, docente, estudiantes y terceros que hagan uso de los sistemas y servicios de comunicación institucional.

3. Principios

- **Uso responsable:** Los recursos tecnológicos deben emplearse únicamente para fines académicos y administrativos.
- **Seguridad:** Se deben aplicar medidas que protejan la información y los sistemas contra accesos no autorizados.
- **Legalidad:** El uso de los sistemas debe cumplir con la normativa vigente en materia de protección de datos y propiedad intelectual.

4. Lineamientos Generales

4.1 Acceso a sistemas

- Cada usuario contará con credenciales únicas e intransferibles.
- Las contraseñas deberán cumplir con requisitos de complejidad y renovarse periódicamente.
- Está prohibido compartir credenciales con terceros.

4.2 Uso de correo electrónico y comunicaciones

- El correo institucional debe utilizarse exclusivamente para actividades académicas y administrativas.
- Queda prohibido el envío de mensajes ofensivos, spam o información no relacionada con las funciones institucionales.
- Se recomienda el uso de cifrado en comunicaciones sensibles.

4.3 Uso de internet y redes

- El acceso a internet debe destinarse a actividades educativas y laborales.
- Se restringirá el acceso a sitios web que representen riesgos de seguridad o que no estén relacionados con las funciones institucionales.
- Está prohibido el uso de la red institucional para descargas ilegales o actividades ilícitas.

4.4 Uso de equipos y software

- Los equipos de cómputo son propiedad institucional y deben cuidarse adecuadamente.
- Está prohibida la instalación de software no autorizado.
- Todo equipo debe contar con antivirus actualizado y parches de seguridad instalados.

4.5 Dispositivos externos y almacenamiento

- El uso de memorias USB, discos externos u otros dispositivos deberá ser autorizado por el área de TI.
- Se recomienda el uso de almacenamiento institucional en servidores o plataformas autorizadas.

4.6 Respaldo y protección de datos

- Los usuarios deberán guardar información crítica en los sistemas institucionales.
- El área de TI realizará respaldos periódicos de datos relevantes.

4.7 Conducta de los usuarios

- Los usuarios deben respetar la privacidad y los derechos de otros.
- Está prohibido acceder, modificar o eliminar información sin autorización.
- Todo incidente de seguridad debe reportarse inmediatamente al área de TI.

5. Responsabilidades

- **Dirección General:** Supervisar el cumplimiento de los lineamientos.
- **Área de TI:** Implementar controles, monitorear el uso de sistemas y atender incidentes.
- **Usuarios:** Cumplir con las normas establecidas y reportar irregularidades.

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