

Lineamientos de Uso de Sistemas y Comunicaciones

Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila

(CECyTE Coahuila)

1. Objetivo

El propósito de este documento es regular el uso de los sistemas informáticos, redes de comunicación y recursos tecnológicos del CECyTE Coahuila, con el objetivo de asegurar su constante disponibilidad, proteger su seguridad y promover su correcto funcionamiento.

2. Alcance

Las disposiciones aquí señaladas aplican a todo el personal administrativo, docente, estudiantes y terceros que hagan uso de los sistemas y servicios de comunicación institucional proporcionados por el colegio.

3. Principios

- **Uso responsable:** Los recursos tecnológicos deben emplearse únicamente para fines académicos y administrativos, evitando su uso para actividades personales o ajenas a la institución.
- **Seguridad:** Es obligación tomar las medidas necesarias para proteger tanto la información como los sistemas institucionales contra accesos no autorizados, salvaguardando la integridad de los datos.
- **Legalidad:** El uso de los sistemas debe estar alineado con la normativa vigente en materia de protección de datos y propiedad intelectual, asegurando el cumplimiento de las leyes aplicables.

4. Lineamientos Generales

4.1 Acceso a sistemas

- Cada usuario contará con credenciales únicas e intransferibles para acceder a los sistemas institucionales.
- Las contraseñas deberán cumplir con requisitos de complejidad y renovarse periódicamente para fortalecer la seguridad.
- Está estrictamente prohibido compartir credenciales con terceros, garantizando la responsabilidad personal sobre el acceso.

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, con el fin de proteger la información confidencial.

4.3 Uso de internet y redes

- El acceso a internet debe destinarse a actividades educativas y laborales, evitando el uso para fines personales o ajenos a la institución.
- 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 cualquier actividad ilícita.

4.4 Uso de equipos y software

- Los equipos de cómputo son propiedad institucional y deben cuidarse adecuadamente para mantener su funcionalidad.
- Está prohibida la instalación de software no autorizado en los equipos institucionales.
- Todo equipo debe contar con antivirus actualizado y parches de seguridad instalados para prevenir incidentes.

4.5 Dispositivos externos y almacenamiento

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

4.6 Respaldo y protección de datos

- Los usuarios deberán guardar información crítica en los sistemas institucionales, evitando almacenar datos sensibles en dispositivos personales.

- El área de TI realizará respaldos periódicos de datos relevantes para garantizar su protección y recuperación ante cualquier eventualidad.

4.7 Conducta de los usuarios

- Los usuarios deben respetar la privacidad y los derechos de otros miembros de la comunidad institucional.
- Está prohibido acceder, modificar o eliminar información sin la debida autorización.
- Todo incidente de seguridad debe reportarse inmediatamente al área de TI, para su atención y resolución adecuada.

5. Responsabilidades

- **Dirección General:** Supervisar el cumplimiento de los lineamientos establecidos en este documento.
- **Área de TI:** Implementar controles de seguridad, monitorear el uso de sistemas y atender cualquier incidente relacionado con los sistemas informáticos.
- **Usuarios:** Cumplir con las normas establecidas y reportar cualquier irregularidad observada durante el uso de los sistemas y recursos tecnológicos.

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