# Política de Seguridad de la Información
# Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila (CECyTE Coahuila)

## 1. Objetivo

Establecer lineamientos y controles que garanticen la confidencialidad, integridad y disponibilidad de la información institucional, así como la protección de los sistemas informáticos y de comunicaciones del CECyTEC Coahuila.

## 2. Alcance

Aplica a todo el personal administrativo, docente, estudiantes y terceros que tengan acceso a los sistemas, programas, datos y equipos de cómputo de la institución.

## 3. Principios

- **Confidencialidad:** La información sensible solo será accesible a personal autorizado.
- **Integridad:** Los datos deben mantenerse completos, exactos y libres de alteraciones no autorizadas.
- **Disponibilidad:** Los sistemas y servicios estarán disponibles de manera continua para cumplir con las funciones académicas y administrativas.

## 4. Lineamientos Generales

- **Gestión de accesos:**
  - Todo usuario debe contar con credenciales únicas (usuario y contraseña).
  - Las contraseñas deberán cumplir con requisitos mínimos de complejidad y renovarse periódicamente.
- **Protección contra accesos no autorizados:**
  - Se implementarán firewalls, sistemas de detección y prevención de intrusos.
  - Se monitorearán intentos de acceso indebido.
- **Uso de antivirus y actualizaciones:**
  - Todos los equipos deberán contar con software antivirus actualizado.
  - El área de TI garantizará la instalación de parches y actualizaciones de seguridad en sistemas y aplicaciones.

- **Respaldo y recuperación:**
  - Se realizarán respaldos periódicos de información crítica.
  - Se establecerán planes de recuperación ante incidentes y desastres.
- **Uso aceptable de recursos:**
  - Los sistemas informáticos y de comunicaciones se utilizarán exclusivamente para fines académicos y administrativos.
  - Queda prohibido instalar software no autorizado.
- **Concientización y capacitación:**
  - El personal recibirá capacitación periódica en temas de seguridad de la información.

**5. Responsabilidades**

- **Dirección General:** Aprobar y supervisar la aplicación de esta política.
- **Área de Tecnologías de la Información:** Implementar controles técnicos y administrativos.
- **Usuarios:** Cumplir con los lineamientos establecidos y reportar incidentes de seguridad.

**6. Vigencia**

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

**Última actualización:** 04 de febrero de 2026