Plan de Recuperación de Desastres y Continuidad de la Operación
Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila
(CECyTE Coahuila)

1. Objetivo

Establecer procedimientos y estrategias para garantizar la continuidad de las operaciones académicas y administrativas del CECyTE Coahuila en caso de desastres naturales, fallas técnicas, ataques informáticos u otros incidentes que afecten la infraestructura tecnológica y física.

2. Alcance

Este plan aplica a:

- **Datos críticos:** bases de datos académicas, administrativas y financieras.
- **Hardware y software críticos:** servidores, equipos de cómputo, aplicaciones institucionales.
- **Personal:** roles y responsabilidades en la atención de incidentes.
- **Espacios físicos:** aulas, oficinas administrativas, centros de cómputo y servidores.

3. Principios

- **Prevención:** Reducir riesgos mediante medidas de seguridad y mantenimiento.
- **Preparación:** Definir protocolos claros para actuar en caso de incidentes.
- **Respuesta:** Atender de manera inmediata y organizada cualquier contingencia.
- **Recuperación:** Restablecer operaciones en el menor tiempo posible.
- **Continuidad:** Mantener servicios esenciales aun en situaciones de emergencia.

4. Estrategias de Recuperación

4.1 Datos

- Respaldo diario de información crítica en servidores internos.
- Copias externas en nube institucional o centro alterno.
- Pruebas trimestrales de restauración de datos.

4.2 Hardware y Software

- Inventario actualizado de equipos y aplicaciones críticas.
- Protocolos de sustitución rápida de hardware dañado.
- Instalación inmediata de software en equipos de reemplazo.

4.3 Personal

- Definición de un **Comité de Continuidad Operativa** integrado por Dirección General, Área de TI y responsables académicos.
- Capacitación anual en protocolos de recuperación y continuidad.
- Roles específicos: detección, notificación, contención, recuperación y documentación.

4.4 Espacios Físicos

- Identificación de áreas críticas y planes de contingencia para su reubicación.
- Uso de espacios alternos en caso de afectación de aulas o centros de cómputo.
- Protocolos de seguridad física (control de acceso, protección contra incendios, energía de respaldo).

5. Procedimientos ante Incidentes

1. **Detección:** Identificación del desastre o incidente.
2. **Notificación:** Reporte inmediato al Comité de Continuidad Operativa.
3. **Evaluación:** Determinar alcance y priorizar servicios críticos.
4. **Contención:** Aislar sistemas afectados y proteger datos.
5. **Recuperación:** Restaurar servicios mediante respaldos y equipos alternos.
6. **Validación:** Confirmar funcionamiento correcto de sistemas y espacios.
7. **Documentación:** Registrar el incidente y las acciones aplicadas.

6. Responsabilidades

- **Dirección General:** Aprobar y supervisar el plan.
- **Área de TI:** Implementar medidas técnicas y coordinar recuperación.
- **Usuarios:** Cumplir protocolos y reportar incidentes oportunamente.

7. 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