

Medidas de Respaldo y Recuperación ante Incidentes

Colegio de Estudios Científicos y Tecnológicos del Estado de Coahuila (CECyTE Coahuila)

1. Objetivo

El propósito de este documento es definir las medidas de respaldo y recuperación de la información, asegurando la continuidad de las operaciones académicas y administrativas del CECyTE Coahuila ante posibles incidentes de seguridad informática, fallas técnicas o desastres. La implementación de estas acciones permite que el instituto esté preparado para enfrentar cualquier situación adversa que pueda afectar sus sistemas.

2. Alcance

Las disposiciones aquí contenidas aplican a todos los sistemas informáticos, servidores, aplicaciones y datos institucionales. Además, involucran a todo el personal administrativo, docente y estudiantes que utilicen dichos sistemas, garantizando que la protección de la información y los mecanismos de recuperación sean responsabilidad compartida por todos los usuarios de la infraestructura tecnológica del CECyTE Coahuila.

3. Principios

Las medidas de respaldo y recuperación se fundamentan en los siguientes principios:

- **Prevención:** Consiste en realizar respaldos periódicos de la información crítica para evitar pérdidas ante cualquier eventualidad.
- **Disponibilidad:** Se busca asegurar que los datos estén accesibles y puedan recuperarse en el menor tiempo posible cuando sea necesario.
- **Integridad:** Es prioritario garantizar que los respaldos generados sean completos y que no presenten alteraciones que puedan comprometer la información.
- **Continuidad:** El objetivo es mantener la operación institucional, incluso ante situaciones de emergencia que pudieran interrumpir el funcionamiento normal.

4. Medidas de Respaldo

4.1 Frecuencia de respaldos

La frecuencia de los respaldos se determina según la importancia y criticidad de la información:

- Las bases de datos críticas deben ser respaldadas de manera **diaria** para asegurar la disponibilidad de los datos más actuales.
- Los archivos administrativos y académicos serán respaldados de forma **semanal**, permitiendo mantener registros actualizados de la gestión institucional.
- Un respaldo **mensual** de los sistemas completos, incluyendo imagen de servidores, garantiza que ante una contingencia mayor se pueda restaurar la infraestructura tecnológica.

4.2 Almacenamiento de respaldos

Para proteger la información respaldada, se establecen los siguientes lineamientos de almacenamiento:

- Los respaldos serán almacenados en servidores seguros ubicados dentro de las instalaciones de la institución.
- Se conservará una copia externa en un centro de datos alternativo o en la nube institucional, brindando una protección adicional en caso de desastres locales.
- Todos los respaldos deben estar cifrados para asegurar la confidencialidad y protección de la información frente a accesos no autorizados.

4.3 Verificación de respaldos

La integridad y funcionalidad de los respaldos se verifica mediante pruebas periódicas:

- Se realizarán pruebas trimestrales para comprobar que los respaldos pueden ser restaurados correctamente y que la información no presenta alteraciones.
- El área de TI será responsable de documentar los resultados de estas pruebas en una bitácora oficial, lo que permitirá dar seguimiento y garantizar la confiabilidad del proceso de respaldo.

5. Medidas de Recuperación

5.1 Procedimiento de recuperación

El procedimiento para recuperar la información y los sistemas ante un incidente consta de las siguientes etapas:

- **Detección:** Identificación del incidente, ya sea por fallo técnico, ataque informático o desastre natural.

- **Notificación:** Reporte inmediato del incidente al área de TI para iniciar el proceso de recuperación.
- **Evaluación:** Determinación del alcance del daño y selección del respaldo más reciente disponible para restablecer la información.
- **Restauración:** Recuperación de los sistemas afectados utilizando los respaldos verificados que garanticen la integridad de la información.
- **Validación:** Confirmación de que los sistemas restaurados funcionan correctamente y cumplen con los estándares operativos.

5.2 Plan de continuidad

Durante el proceso de recuperación, se implementan acciones para asegurar la continuidad de las operaciones institucionales:

- Se establecerán procedimientos alternativos que permitan mantener las funciones esenciales mientras se realiza la recuperación de los sistemas.
- El área de TI, en coordinación con la Dirección General, priorizará la restauración de los servicios críticos para minimizar el impacto en la institución.

6. Responsabilidades

Las responsabilidades en la implementación de las medidas de respaldo y recuperación se asignan de la siguiente manera:

- **Dirección General:** Aprobar y supervisar la aplicación de las medidas descritas en este documento, asegurando su cumplimiento.
- **Área de TI:** Llevar a cabo los respaldos, realizar pruebas de recuperación y coordinar las acciones necesarias ante la ocurrencia de incidentes.
- **Usuarios:** Utilizar los sistemas institucionales para guardar información y reportar oportunamente cualquier incidente que pueda afectar la seguridad de los datos.

7. Vigencia

Este documento entra en vigor el **04 de febrero de 2026** y será revisado de manera anual, o cuando se presenten cambios relevantes en la infraestructura tecnológica o en la normativa aplicable, asegurando que las medidas adoptadas se mantengan actualizadas y efectivas.

Última actualización: 04 de febrero de 2026