PLAN DE RESPALDO

# Objetivo

Definir las estrategias, procedimientos y herramientas necesarias para realizar copias de seguridad de la información crítica del sistema Gestión de Certificados CMC, garantizando la recuperación en caso de pérdida de datos, errores de configuración, ataques o fallos del sistema.

# Alcance

Este plan aplica al backend del sistema CMC, su base de datos MySQL, archivos de configuración (.env) y cualquier archivo adjunto a certificados emitidos. Se aplica a entornos de desarrollo, pruebas y producción.

# Elementos a respaldar

- Base de datos MySQL (estructura y contenido).  
- Archivo .env del backend.  
- Código fuente del sistema.  
- Archivos estáticos de certificados, si se almacenan localmente.

# Frecuencia del respaldo

- Diario: respaldo automático de la base de datos en entornos de producción.  
- Semanal: respaldo completo del sistema, incluyendo configuración y archivos del backend.  
- Mensual: respaldo archivado en almacenamiento externo o nube.  
- Antes de cualquier actualización o migración importante: respaldo manual completo.

# Procedimiento de respaldo manual

1. Acceder al servidor con permisos de administrador.  
2. Realizar respaldo de la base de datos con:  
 `mysqldump -u usuario -p certificados\_db > respaldo.sql`  
3. Copiar el archivo .env con:  
 `cp .env respaldo\_env.txt`  
4. Comprimir el respaldo:  
 `tar -czvf respaldo\_completo.tar.gz respaldo.sql respaldo\_env.txt`  
5. Guardar el archivo en una carpeta segura o servidor externo.  
6. Registrar en bitácora de respaldos la fecha, hora y contenido del respaldo.

# Procedimiento de restauración

1. Descomprimir el respaldo:  
 `tar -xzvf respaldo\_completo.tar.gz`  
2. Restaurar la base de datos:  
 `mysql -u usuario -p certificados\_db < respaldo.sql`  
3. Reemplazar el archivo .env si es necesario:  
 `cp respaldo\_env.txt .env`  
4. Reiniciar el backend:  
 `bun start` o `npm start`  
5. Verificar conexión con la base de datos y que el sistema funcione normalmente.

# Herramientas recomendadas

- `mysqldump` y `mysql` para respaldo y restauración.  
- `cron` para automatizar respaldos diarios.  
- `rsync` o almacenamiento en nube (Google Drive, AWS S3, etc.)  
- Repositorio Git para código fuente y configuración (sin claves en texto plano).

# Responsables

El responsable técnico del sistema deberá:  
- Ejecutar respaldos manuales antes de actualizaciones.  
- Asegurar que los respaldos automáticos se ejecutan correctamente.  
- Validar restauraciones periódicas de prueba.  
- Custodiar las copias de seguridad en ubicaciones seguras.