INSTITUTO POLITÉCNICO NACIONAL

UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA Y CIENCIAS SOCIALES Y ADMINISTRATIVAS

Plan de Recuperación ante Desastres (DRP) para la Base de Datos "BD_Gimnasio"

P R E S E N T A

Mora Flores Omar

Lugo Mora José Yael

Ramírez Ramos Ángel Jair

Ramírez Blas Luis Ángel

Trejo Monroy Stefany

Profesor

MTRO. Martínez Vázquez Gustavo

CIUDAD DE MÉXICO, MÉXICO **2025**

Plan de Recuperación ante Desastres (DRP)

Documento:	**Plan de Recuperación de Desastres (DRP)**
Activo Crítico:	Base de Datos BD_Gimnasio
Versión:	2.0
Fecha de Aprobación:	11 de junio de 2025
Próxima Revisión:	11 de junio de 2026
Propietario del Plan:	Departamento de TI

1. Resumen Ejecutivo

Este documento establece la estrategia, los protocolos y las responsabilidades para la recuperación efectiva y oportuna de la base de datos BD_Gimnasio tras un incidente disruptivo. La integridad y disponibilidad de esta base de datos son **críticas** para todas las operaciones del negocio, incluyendo el control de acceso de miembros, la gestión de pagos, la seguridad de las instalaciones y la administración general.

El plan está diseñado para cumplir con los siguientes objetivos de negocio, definidos en colaboración con la dirección:

- **RPO (Objetivo de Punto de Recuperación): 15 minutos.** El negocio no puede tolerar una pérdida de datos superior a 15 minutos.
- **RTO (Objetivo de Tiempo de Recuperación): 2 horas.** El sistema de base de datos debe estar completamente funcional en un nuevo entorno dentro de las 2 horas posteriores a la declaración oficial del desastre.

2. Equipo de Recuperación y Responsabilidades

Rol	Nombre/Contacto	Responsabilidades Clave Durante un Incidente

Líder del Equipo de Recuperación	[Nombre del Gerente de TI]	- Activar el DRP. - Coordinar a todo el equipo. - Tomar decisiones críticas. - Comunicarse con la alta dirección.
Administrador de BD (DBA)	[Nombre del DBA Principal]	- Ejecutar los scripts de restauración. - Validar la integridad de los datos (DBCC CHECKDB). - Confirmar la consistencia de la BD post-recuperación.
Administrador de Sistemas	[Nombre del SysAdmin]	- Aprovisionar hardware (servidores físicos o virtuales). - Instalar y configurar el S.O. y SQL Server. - Configurar la red y la seguridad del nuevo servidor.
Especialista de Aplicaciones	[Nombre del Desarrollador]	- Reconfigurar las cadenas de conexión. - Probar la funcionalidad de las aplicaciones (control de acceso, CRM). - Desplegar parches si es necesario.
Líder de Comunicaciones	[Nombre del Gerente General]	- Ejecutar el plan de comunicaciones. - Informar al personal y a los gerentes sobre el estado del sistema.

3. Criterios de Activación del Plan

Este DRP se activará oficialmente por el **Líder del Equipo de Recuperación** si se cumple **uno o más** de los siguientes criterios:

- **Corrupción de Datos Grave:** DBCC CHECKDB reporta errores irreparables que afectan a tablas críticas (miembros, accesos).
- **Fallo de Hardware Crítico:** El servidor de la base de datos principal sufre un fallo irrecuperable (ej. fallo de la placa base, fallo del arreglo de almacenamiento RAID).
- **Pérdida de Acceso al Servidor:** Imposibilidad de conectar con el servidor de producción por más de 30 minutos sin una causa de red identificada.
- **Incidente de Seguridad Mayor:** Un ciberataque (ej. ransomware) cifra o destruye los datos de la base de datos.
- **Desastre Físico:** El centro de datos principal queda inaccesible o destruido (incendio, inundación, etc.).

4. Estrategia Detallada de Copias de Seguridad

Para cumplir el RPO, el modelo de recuperación de BD_Gimnasio está configurado en **FULL**. Las copias de seguridad se automatizan mediante **SQL Server Agent Jobs**.

4.1. Tipos y Frecuencia

- **Backup Completo:**
  - **Cuándo:** Cada domingo a las 02:00.
  - **Nomenclatura:** BD_Gimnasio_FULL_YYYYMMDD_HHMM.bak
  - **Retención:** 4 semanas (en almacenamiento local y de red), 1 año (en la nube).
- **Backup Diferencial:**
  - **Cuándo:** Diario (Lunes a Sábado) a las 22:00.
  - **Nomenclatura:** BD_Gimnasio_DIFF_YYYYMMDD_HHMM.bak
  - **Retención:** 14 días (local/red).
- **Backup de Log de Transacciones:**
  - **Cuándo:** Cada 15 minutos, de Lunes a Domingo, entre las 05:00 y las 23:59.
  - **Nomenclatura:** BD_Gimnasio_LOG_YYYYMMDD_HHMM.trn
  - **Retención:** 72 horas (local/red).

4.2. Validación y Almacenamiento

- **Validación:** Todas las tareas de backup utilizan la opción WITH CHECKSUM para garantizar la integridad. Adicionalmente, se ejecuta un script diario que realiza un RESTORE VERIFYONLY en el último conjunto de backups.
- **Almacenamiento (Regla 3-2-1):**

1. **Copia 1 (Local):** En un disco duro separado en el mismo servidor para restauraciones ultrarrápidas.
2. **Copia 2 (Red):** En un dispositivo NAS en una ubicación de red diferente dentro del mismo edificio.
3. **Copia 3 (Off-Site):** Replicación diaria de la copia del NAS a una cuenta de **Azure Blob Storage (Cool Tier)** para protección geográfica.

5. Procedimientos Detallados de Restauración (Playbooks)

Playbook 1: Restauración a un Punto en el Tiempo (Error Humano / Corrupción Leve)

1. **ACCIÓN (Líder):** Poner las aplicaciones en modo "mantenimiento".
2. **ACCIÓN (DBA):** Identificar la marca de tiempo exacta **antes** del evento.
3. **ACCIÓN (DBA):** Realizar un último backup del final del log WITH NORECOVERY para capturar las últimas transacciones no respaldadas.
   ```
   BACKUP LOG BD_Gimnasio TO DISK = '...' WITH NORECOVERY;
   ```
4. **ACCIÓN (DBA):** Ejecutar el script de restauración:
   ```
   -- Restaurar el último FULL sin poner la BD en línea
   RESTORE DATABASE BD_Gimnasio FROM DISK = '...' WITH NORECOVERY, REPLACE;
   -- Restaurar el último DIFFERENTIAL
   RESTORE DATABASE BD_Gimnasio FROM DISK = '...' WITH NORECOVERY;
   -- Aplicar todos los LOGS en secuencia
   RESTORE LOG BD_Gimnasio FROM DISK = '...' WITH NORECOVERY;
   RESTORE LOG BD_Gimnasio FROM DISK = '...' WITH NORECOVERY;
   -- Aplicar el último LOG especificando el punto de corte en el tiempo
   RESTORE LOG BD_Gimnasio FROM DISK = '...' WITH STOPAT = 'YYYY-MM-DDTHH:MM:SS', RECOVERY;
   ```

5. **ACCIÓN (DBA/Especialista App):** Ejecutar el checklist de verificación post-recuperación.

Playbook 2: Recuperación por Pérdida Total del Servidor (Fallo de Hardware)

1. **ACCIÓN (Líder):** Activar el DRP y convocar al equipo de recuperación.
2. **ACCIÓN (Admin. Sistemas):** Aprovisionar un nuevo servidor (físico o VM) según las especificaciones documentadas.
3. **ACCIÓN (Admin. Sistemas):** Instalar S.O. y SQL Server con la misma versión y *collation* que el servidor original.
4. **ACCIÓN (Admin. Sistemas):** Configurar red, firewall y políticas de seguridad.
5. **ACCIÓN (DBA):** Copiar el conjunto de backups más reciente desde el NAS o la nube al nuevo servidor.
6. **ACCIÓN (DBA):** Ejecutar el proceso de restauración completo (Full + Diff + todos los Logs) finalizando con WITH RECOVERY.
7. **ACCIÓN (DBA):** Sincronizar los inicios de sesión (logins) del servidor usando scripts pre-generados o herramientas como sp_help_revlogin.
8. **ACCIÓN (Especialista App):** Actualizar las entradas DNS y/o las cadenas de conexión de las aplicaciones para que apunten al nuevo servidor.
9. **ACCIÓN (Todo el Equipo):** Realizar pruebas exhaustivas de funcionalidad de extremo a extremo.

6. Verificación y Cierre del Incidente

1. **Verificación Técnica:**

- DBCC CHECKDB('BD_Gimnasio') WITH NO_INFOMSGS, ALL_ERRORMSGS; -> Debe devolver cero errores.
- Verificar el número de filas en tablas clave.
- Confirmar que los últimos registros de la tabla accesos son consistentes con el RPO.

2. **Verificación Funcional:**

- Un gerente debe poder iniciar sesión en el panel de administración.
- Registrar un nuevo miembro de prueba.
- Simular un acceso (ingreso/salida) y verificar que se registre.

3. **Cierre:**

   - El Líder del Equipo de Recuperación declara formalmente el fin del desastre.
   - Se completa un **Análisis de Causa Raíz (RCA)** en las 48 horas posteriores para documentar el incidente, las lecciones aprendidas y las acciones para prevenir su recurrencia.

7. Mantenimiento y Pruebas del Plan

- **Simulacros Teóricos (Tabletop Exercise):** Trimestralmente, el equipo se reúne para discutir un escenario de desastre hipotético y revisar los pasos del plan.
- **Pruebas de Restauración Completas:** Semestralmente, se restaura una copia completa de la base de datos en un entorno de pruebas aislado para validar los backups y cronometrar el proceso de recuperación (medir el RTO real).
- **Revisión Anual:** Este documento se revisa y se actualiza anualmente, o cuando haya cambios significativos en la infraestructura o el software.