



Backup y Restore

AR Tema extractado del libro "**Análisis Funcional de Sistemas y Tecnologías de la Información**" de Aníbal M. Mazza Fraquelli - ISBN 978-987-26981-3-3

Presentación del Tema

En el entorno digital contemporáneo, donde los procesos organizacionales dependen estructuralmente de los Sistemas de Información (SI – *Information Systems*), la gestión adecuada de **Backup y Restore** constituye uno de los pilares fundamentales de la resiliencia tecnológica. El término *backup* (copia de seguridad) refiere al proceso de generar una copia adicional de los datos con el fin de preservarlos ante pérdida, corrupción o destrucción. El término *restore* (restauración) implica el proceso de recuperar esos datos desde la copia de seguridad hacia su estado operativo.

La correcta implementación de estrategias de backup no es una decisión exclusivamente técnica, sino estratégica. Desde la perspectiva de la administración, el diseño de políticas de respaldo debe alinearse con la criticidad de la información, los objetivos de recuperación, la tolerancia al riesgo y la continuidad del negocio. Una organización puede sobrevivir a múltiples fallas operativas, pero difícilmente sobreviva a la pérdida irreversible de su información crítica.

En este contexto, adquieren relevancia conceptos como la clasificación de datos según su criticidad, los objetivos de recuperación (RTO y RPO), las modalidades de almacenamiento (on premises y on cloud), la estrategia 3-2-1, el concepto de *off-site*, y los distintos tipos de backup (full, incremental y diferencial).

Comprender estas nociones permite a los futuros administradores integrar gobernanza de datos, gestión de riesgos y planificación tecnológica.

Desarrollo

1. Backup y Restore: Concepto y Función

El **backup** consiste en la creación sistemática de copias de información con el propósito de garantizar su disponibilidad ante incidentes tales como:

- Fallas de hardware.
- Errores humanos.
- Ciberataques (ransomware).
- Corrupción de bases de datos.
- Desastres físicos (incendio, inundación).

El **restore** es el proceso mediante el cual se recuperan esos datos desde las copias almacenadas.

Desde el punto de vista organizacional, la efectividad de un backup no se mide por su existencia, sino por su capacidad real de restauración en los tiempos requeridos por el negocio.

2. Clasificación Adecuada de los Datos

No todos los datos poseen el mismo nivel de criticidad. Una estrategia de backup eficiente comienza con la clasificación adecuada de la información.

2.1 Categorías de Clasificación

1. Datos críticos:

- Estados financieros.
- Bases de clientes.
- Sistemas de facturación.
- Información regulada.

2. Datos necesarios:

- Documentación operativa.
- Archivos administrativos.
- Informes internos.

3. **Datos no esenciales:**

- Archivos temporales.
- Datos redundantes.

La clasificación permite asignar:

- Frecuencia de backup.
- Nivel de redundancia.
- Prioridad de restauración.
- Recursos de almacenamiento.

Desde la administración, clasificar datos evita sobredimensionar costos y subdimensionar riesgos.

3. **Objetivos de Recuperación**

Dos conceptos clave orientan la planificación:

- **RTO (Recovery Time Objective / Objetivo de Tiempo de Recuperación):** tiempo máximo aceptable para restaurar un servicio.
- **RPO (Recovery Point Objective / Objetivo de Punto de Recuperación):** máxima pérdida de datos tolerable medida en tiempo.

Ejemplo:

- RTO: 4 horas.
- RPO: 1 hora.

Esto implica que el sistema debe restaurarse en 4 horas y no perder más de una hora de datos.

4. **Modalidades de Backup**

4.1 **Backup On-Premises**

Consiste en almacenar copias dentro de la infraestructura física de la organización.

Ventajas:

- Control directo.
- Acceso rápido.

Desventajas:

- Riesgo físico compartido (incendio, robo).
 - Mayor inversión en hardware.
-

4.2 Backup On-Cloud

Implica almacenar copias en proveedores de nube.

Ventajas:

- Escalabilidad.
- Reducción de infraestructura física.
- Ubicación geográficamente distribuida.

Desventajas:

- Dependencia del proveedor.
- Costos recurrentes.
- Riesgo de conectividad.

La estrategia óptima suele combinar ambos.

5. Estrategia 3-2-1

La estrategia **3-2-1** es una práctica ampliamente recomendada:

- 3 copias de los datos.
- 2 soportes distintos.
- 1 copia fuera del sitio (*off-site*).

Ejemplo:

- Copia principal en servidor productivo.
- Copia secundaria en almacenamiento local.
- Copia adicional en la nube o en otro edificio.

Este enfoque reduce el riesgo de pérdida simultánea.

6. Concepto de Off-Site

El concepto *off-site* implica que al menos una copia debe almacenarse físicamente en una ubicación diferente.

Si el data center principal sufre un incendio, la copia local también podría perderse. La copia off-site garantiza recuperación ante desastres físicos.

7. Clasificación Según Cantidad y Periodicidad

La frecuencia del backup depende de:

- Volumen de transacciones.
- Criticidad del proceso.
- RPO establecido.

Sistemas financieros de alta transaccionalidad pueden requerir backups horarios; otros sistemas pueden tolerar backups diarios o semanales.

8. Tipos de Backup

8.1 Backup Full

Copia completa de todos los datos.

Ventajas:

- Restauración sencilla.
- Integridad total.

Desventajas:

- Mayor tiempo.
 - Mayor espacio de almacenamiento.
-

8.2 Backup Incremental

Copia solo los cambios desde el último backup (sea full o incremental).

Ventajas:

- Menor espacio.
- Mayor rapidez.

Desventajas:

- Restauración más compleja.
-

8.3 Backup Diferencial

Copia los cambios desde el último backup full.

Ventajas:

- Restauración más simple que incremental.
- Menor volumen que full diario.

Desventajas:

- Crece en tamaño a lo largo de la semana.
-

9. Ejemplo Práctico

Supongamos una empresa que realiza:

- **Backup Full cada viernes por la noche.**
- **Backup Incremental cada día (lunes a jueves).**

Esquema semanal:

Viernes: Backup Full

Lunes: Backup Incremental

Martes: Backup Incremental

Miércoles: Backup Incremental

Jueves: Backup Incremental

Si ocurre una falla el jueves:

Se restaura:

1. Backup Full del viernes.
2. Incrementales de lunes, martes, miércoles y jueves.

Este esquema equilibra eficiencia de almacenamiento y capacidad de recuperación.

Alternativamente, podría utilizarse:

- Backup Full semanal.
- Backup Diferencial diario.

En ese caso, la restauración requeriría solo el full más el diferencial más reciente.

10. Riesgos y Errores Comunes

- No probar restauraciones.
- No verificar integridad.
- No cifrar backups.
- No proteger contra ransomware.
- No documentar procedimientos.

Un backup no probado es un riesgo oculto.

11. Dimensión Estratégica

Desde la administración:

- La política de backup debe alinearse con la estrategia de negocio.
- Debe existir presupuesto asignado.
- Debe integrarse con BCP y DRP.
- Debe auditarse periódicamente.

El costo de prevención es inferior al costo de pérdida de datos críticos.

Conclusión

El backup y restore constituyen mecanismos esenciales para garantizar la continuidad y resiliencia de los sistemas de información. La correcta clasificación de los datos, la definición de objetivos de recuperación (RTO y RPO), la implementación de estrategias como 3-2-1, la utilización de almacenamiento on-premises y on-cloud, y la adecuada selección entre backups full, incremental o diferencial permiten construir una arquitectura de protección robusta.

La clave estratégica radica en comprender que la información es un activo crítico. Sin una política de backup adecuada y probada, la organización queda expuesta a pérdidas irreversibles que pueden comprometer su sostenibilidad financiera y reputacional. La gestión responsable del respaldo de datos no es una opción técnica, sino una decisión de gobernanza.

Preguntas de autoevaluación

1. ¿Cuál es la diferencia entre backup full, incremental y diferencial?
 2. ¿Qué implica la estrategia 3-2-1 y por qué es recomendable?
 3. ¿Cómo influyen RTO y RPO en el diseño de la política de backup?
 4. ¿Por qué es importante la clasificación de datos antes de definir la estrategia de respaldo?
 5. ¿Qué ventajas y riesgos presentan los backups on-premises y on-cloud?
-

Material de Clases

Compilado por **Aníbal M. Mazza Fraquelli** Doctor de la Universidad de Buenos Aires para el uso de sus clases en la Facultad de Ciencias Económicas de la Universidad de Buenos Aires.

Contenidos de esta página

Los contenidos **aquí incluidos integran desarrollos y escritos propios del autor, así como materiales de terceros (documentos, textos, fragmentos, conceptos, imágenes, esquemas, definiciones u otros recursos)**, los cuales son utilizados a título ilustrativo, explicativo o formativo, respetando la normativa vigente en materia de derechos de autor y citando las fuentes cuando corresponde.

La selección, organización, adaptación pedagógica y contextualización de los contenidos constituye un trabajo original del autor, orientado a facilitar los procesos de enseñanza y aprendizaje.

Este material no persigue fines comerciales y su reproducción, total o parcial, queda limitada al ámbito educativo, debiendo preservarse siempre la mención de la autoría y las fuentes originales.

Autorización de uso

Se permite la reproducción, comunicación pública, distribución y utilización total o parcial de los contenidos de su material, en formato físico o digital, con fines exclusivamente educativos, académicos o de divulgación, siempre que se respete la integridad del contenido y se incluya la correspondiente referencia a la fuente y a la autoría.

Las ideas, opiniones e interpretaciones contenidas en este material corresponden exclusivamente al autor.

Queda expresamente excluido cualquier uso con fines comerciales.