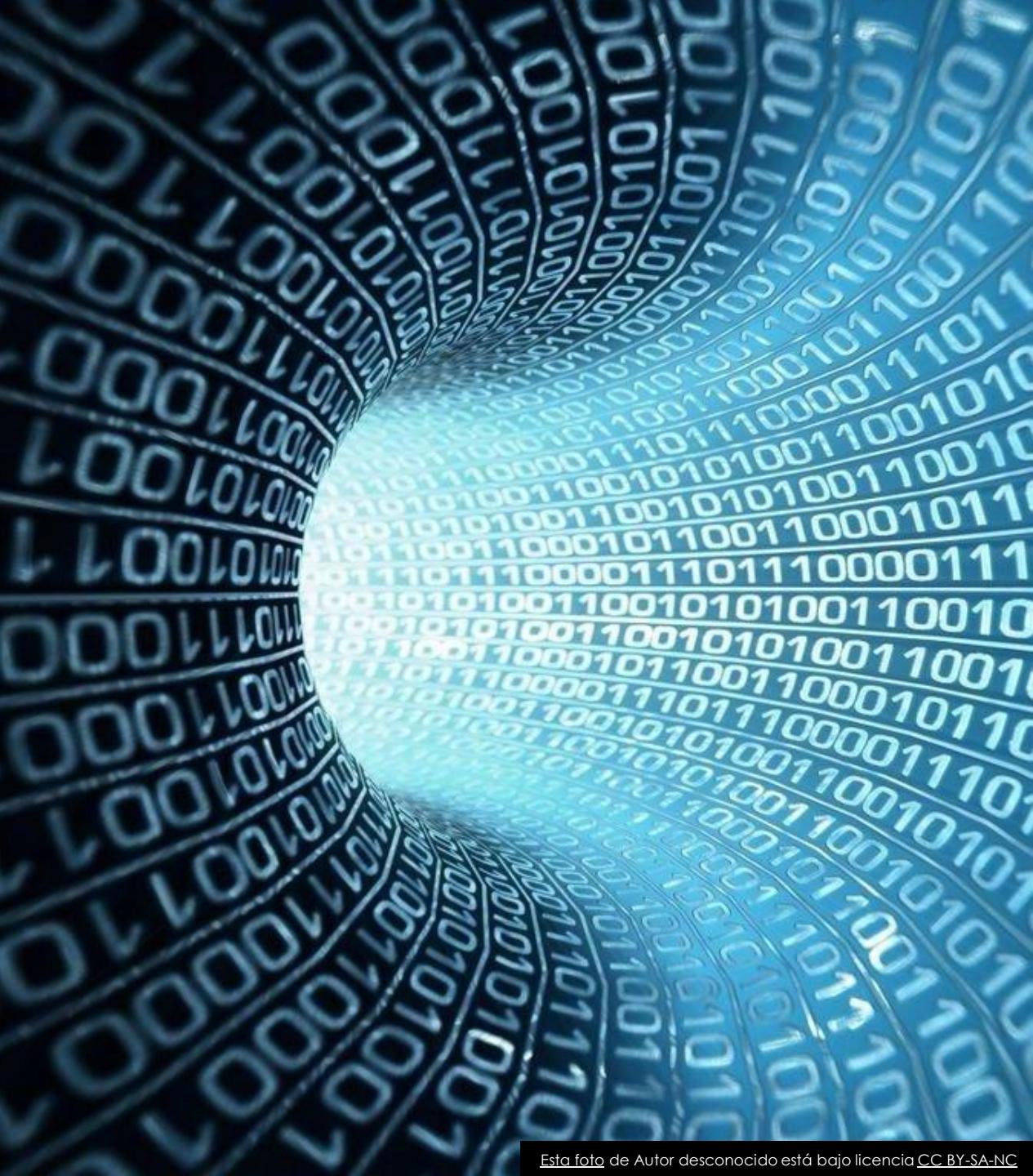


Bases de datos 2

Clase 5

Kevin Morán

bases2.fiusac@gmail.com



Protección de datos y Backup

UNIDAD NO. 3

Definiciones

- Un backup es una copia adicional de la información que puede utilizarse con fines de recuperación y restauración ante fallos.
- Su utilización se hace cuando la copia original **está inutilizada o corrupta**.
- La copia puede ser:
 - Copias de los ficheros en instantes de tiempo determinados.
 - Copias especulares de los datos originales completamente sincronizados.

Tipologías de Backups

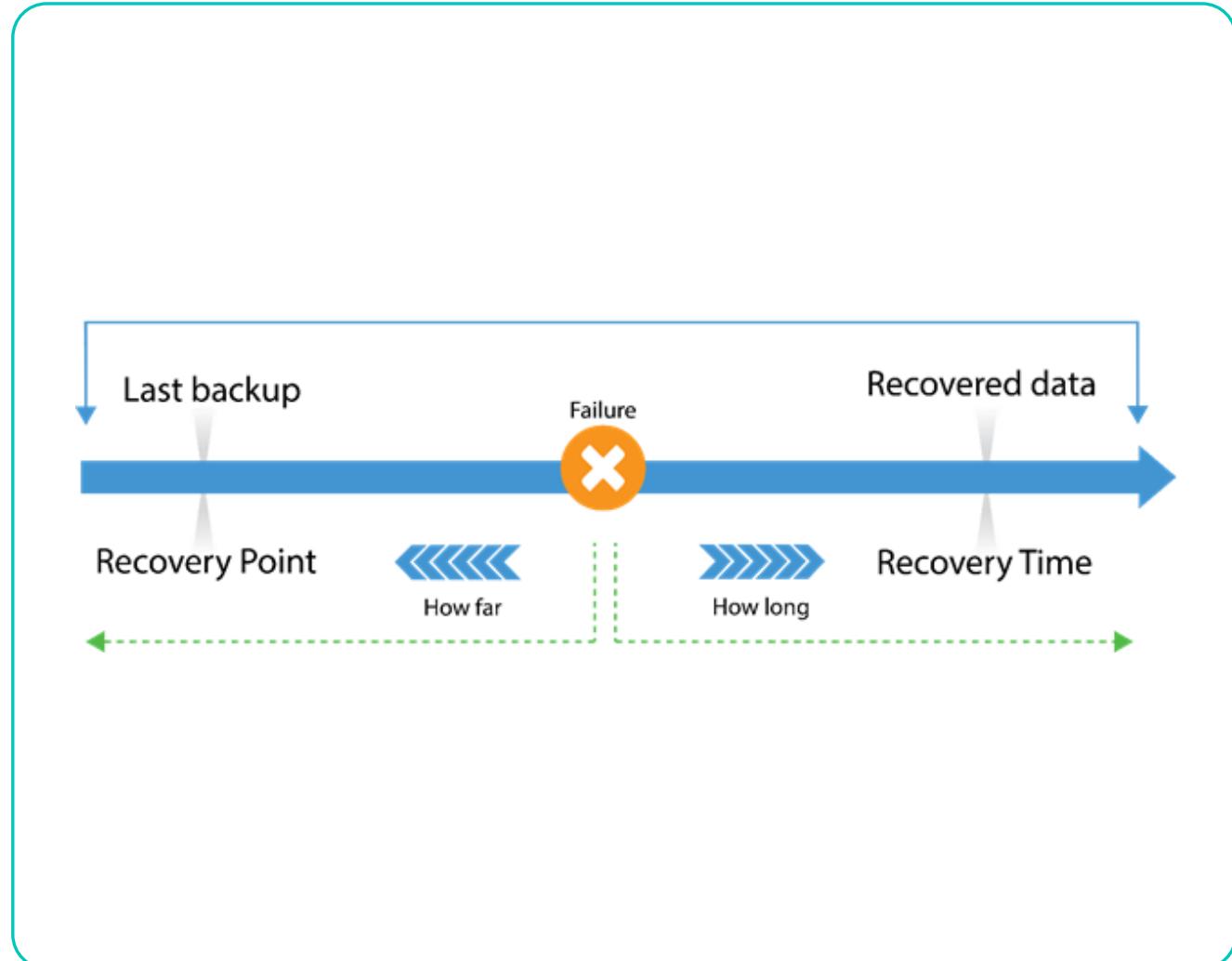
- Según necesidades:
 - Copias para recuperación ante desastres: El objeto es disponer de una copia que subsane la perdida potencial de datos valiosos para el usuario.
 - Copias operacionales: Se hacen para disponer de una instantánea de los datos del sistema en un momento determinado, con la intención de poder regresar a esa situación (sin necesidad de que haya un desastre):
 - E.g., versiones de un repositorio software.
 - Copias reguladas: Se realizan para cumplir con normativas legales que exigen el almacenado de datos históricos durante un periodo de tiempo. (LOPD en España).

Requisitos de usuario

- Plazos de recuperación
- Instalaciones:
 - Original
 - De recuperación
- Elementos a recuperar:
 - Ficheros con poca variación.
 - Ficheros con mucha variación.
- Temporizaciones:
 - Cuándo se hacen los backups.
 - Cuánto tiempo dura la operación de copia.
 - Durante cuánto tiempo se guarda copias.

Plazos de recuperación

- Recovery Point Objective (RPO): Periodo máximo de tiempo en el cual se han podido ver afectados datos antes de un incidente.
- Recovery Time Objective (RTO): Periodo máximo de tiempo en el que es asumible tener los sistemas de información parados después de un incidente.



Planificación de la Organización

- La empresa debe incluir en sus procedimientos internos diferentes documentos de reglamentación:
 - Plan de continuidad del negocio (business continuity plan): Que indica la exposición de la organización a amenazas internas y externas y las contramedidas para prevención y recuperación. Incluye:
 - Análisis de impacto en el negocio (business impact analysis – BIA): Se diferencian sistemas críticos de no críticos y donde se definen, por ejemplo RTP y RPO.
 - Análisis de amenazas y riesgos (threat and risk analysis – TRA): Se identifican los tipos de amenazas.

Planificación de la organización (2)

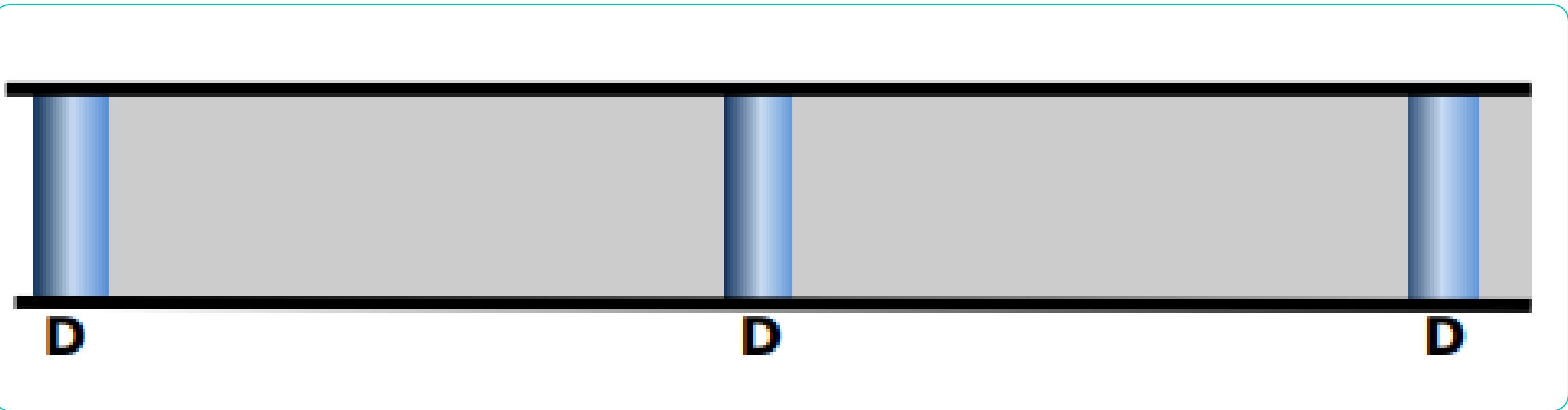
- Plan de recuperación ante desastres (disaster recovery plan): Determina los pasos a realizar para realizar las acciones de recuperación ante un incidente.
 - Incluye las prioridades de esas tareas, el entrenamiento de los grupos participantes y los canales de comunicación.
 - Debe realizarse un **ensayo** de recuperación de forma periódica para verificar la integridad de datos y la agilidad de los procedimientos.
 - Lleva asociado acciones relativas al **inventario** sistemático de equipos, las pólizas de seguro y garantías de los mismos y un listado de números de emergencias y similares.

Tipologías de Backups

- Por Granularidad:
 - “Cuándo y de qué se hace copia”.
 - Se determinan diferentes tipos de backups de acuerdo a cuáles son los ficheros copiados.
 - Los diferentes tipos de backups se hacen en “ciclos de backup”
- Por Operatividad del sistema: – “En qué estado está el sistema cuando se realiza la copia”.
 - Se determina si es necesario detener la operativa del sistema (dejar de proporcionar servicio) para hacer el backup.

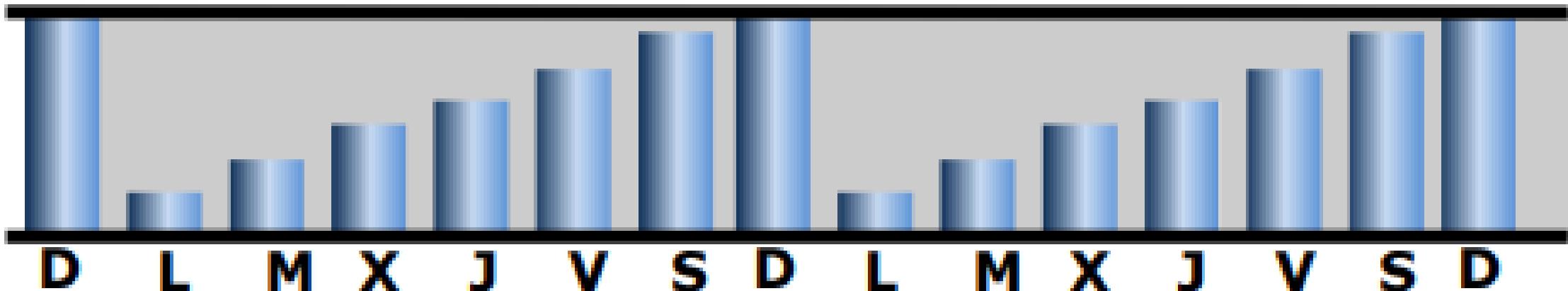
Granularidad





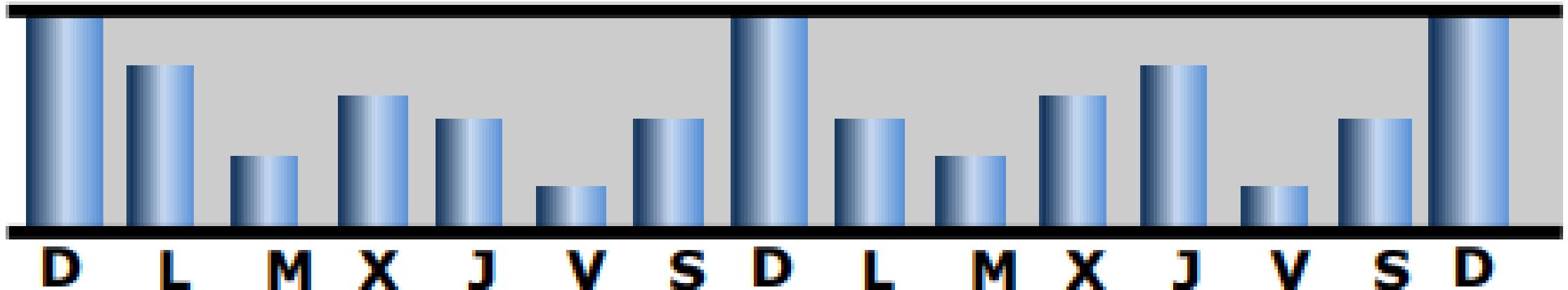
Backup completo

- Se realiza una copia integral de los datos, copiando todos los contenidos de los sistemas a mantener.



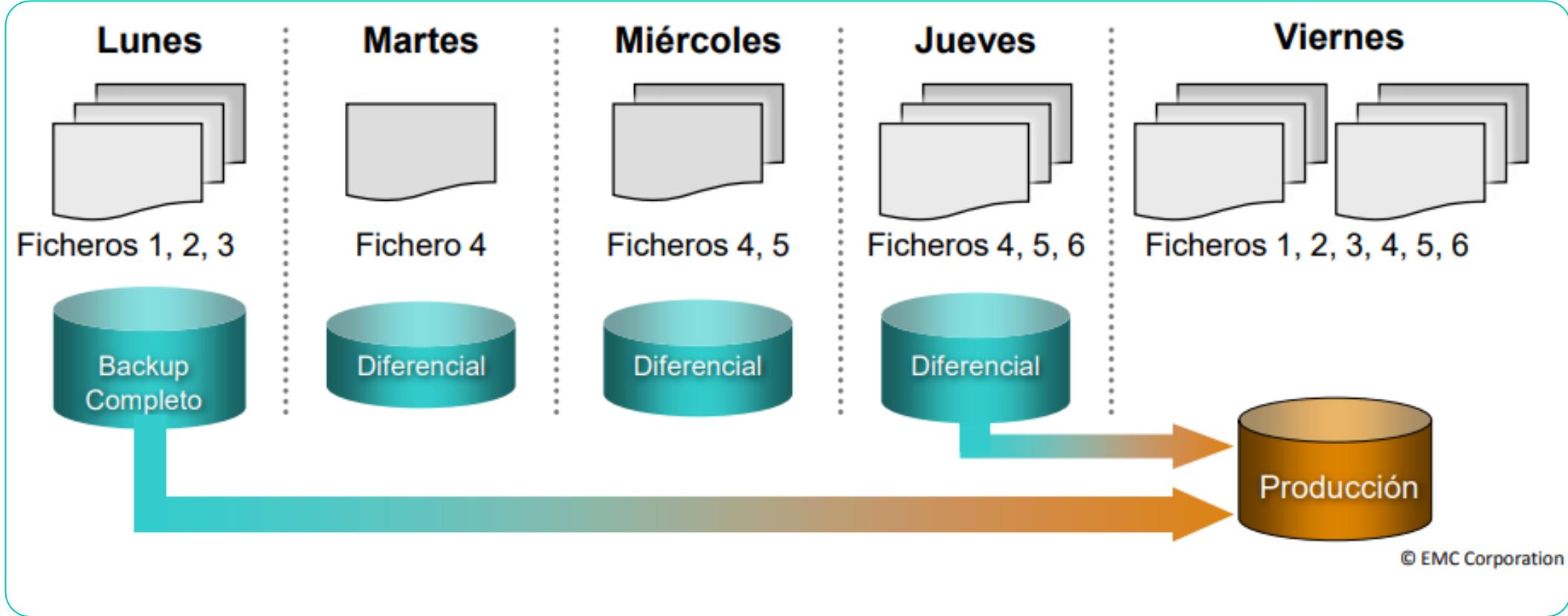
Backup diferencial

- Partiendo de una copia de backup completa, se realiza una copia de todos los datos modificados desde que se hizo ese backup completo.

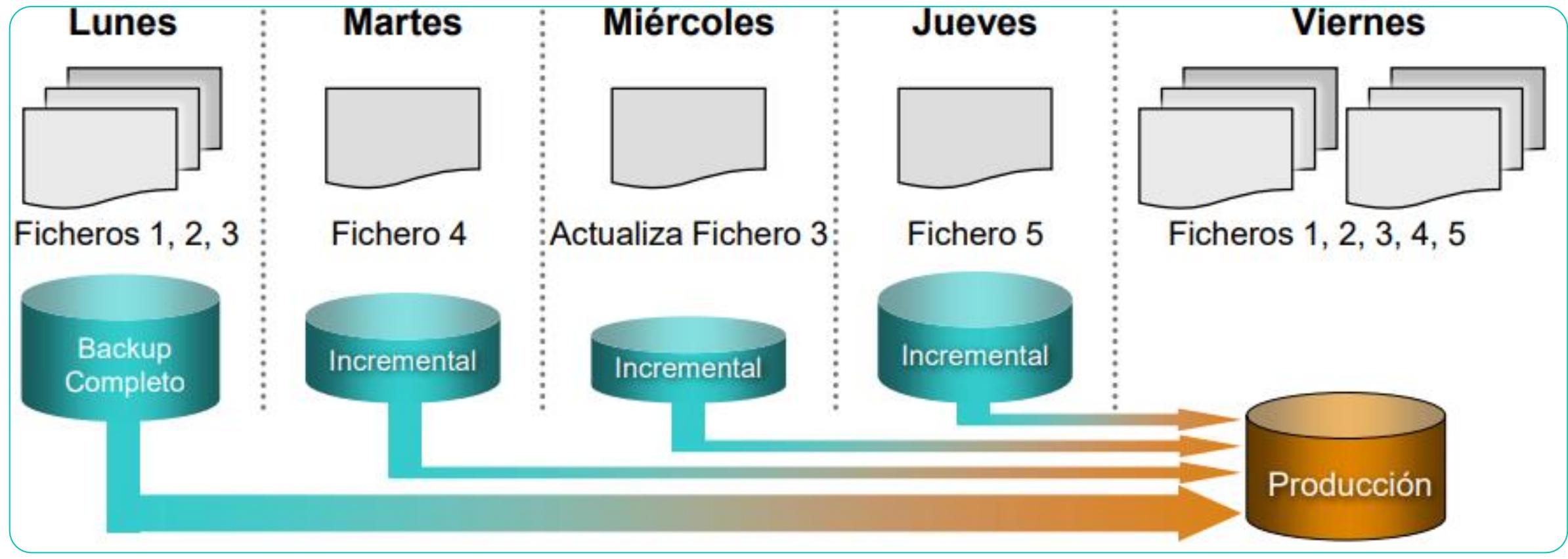


Backup incremental

- Partiendo de una copia de backup completa, se realiza una copia sólo de los datos modificados desde el último backup (sea completo o incremental).



Recuperación de un Backup Diferencial



Recuperación de Backup incremental

Operatividad del sistema durante la copia

Backup frio (cold) u offline

- La operatividad del sistema se detiene
 - Entre el comienzo de la fase de copia y el final de la misma no se hace ninguna operación sobre los datos.
 - Requiere ventanas de tiempo para realizar esas copias que deben ser programadas y validadas.
 - No válido para sistemas 24x7 (e.g., un comercio on-line).

Backup caliente (hot) u on-line

- La operativa del sistema no se detiene y la copia se hace con el sistema en producción.
 - Requiere fijar el instante de tiempo de referencia.
 - Gestionar no sólo datos estables sino las modificaciones (log de operaciones) entre ese instante y el final de la copia.
- Proceso:
 - Se configura el sistema en modo hot backup
 - Se crea un log de operaciones donde se almacenan todas las modificaciones que se piden sobre los datos al comenzar la copia:
 - Eso implica que los datos estables no se modifican por esas operaciones.
 - Al finalizar la copia el redo log se ejecuta y se aplican todos los cambios.

RMAN

Types of failures

- Instance Failure
 - Usually connected with an Oracle process failure
- Media Failure
 - Disk failure, storage array controller failure etc.
- Block Corruption
 - Usually caused by bugs in Oracle software
- Human error
 - In most cases accidentally deleted/updated data
 - Database user or DBA
- Disaster
 - Fire, flood, earthquake, plane crash etc.

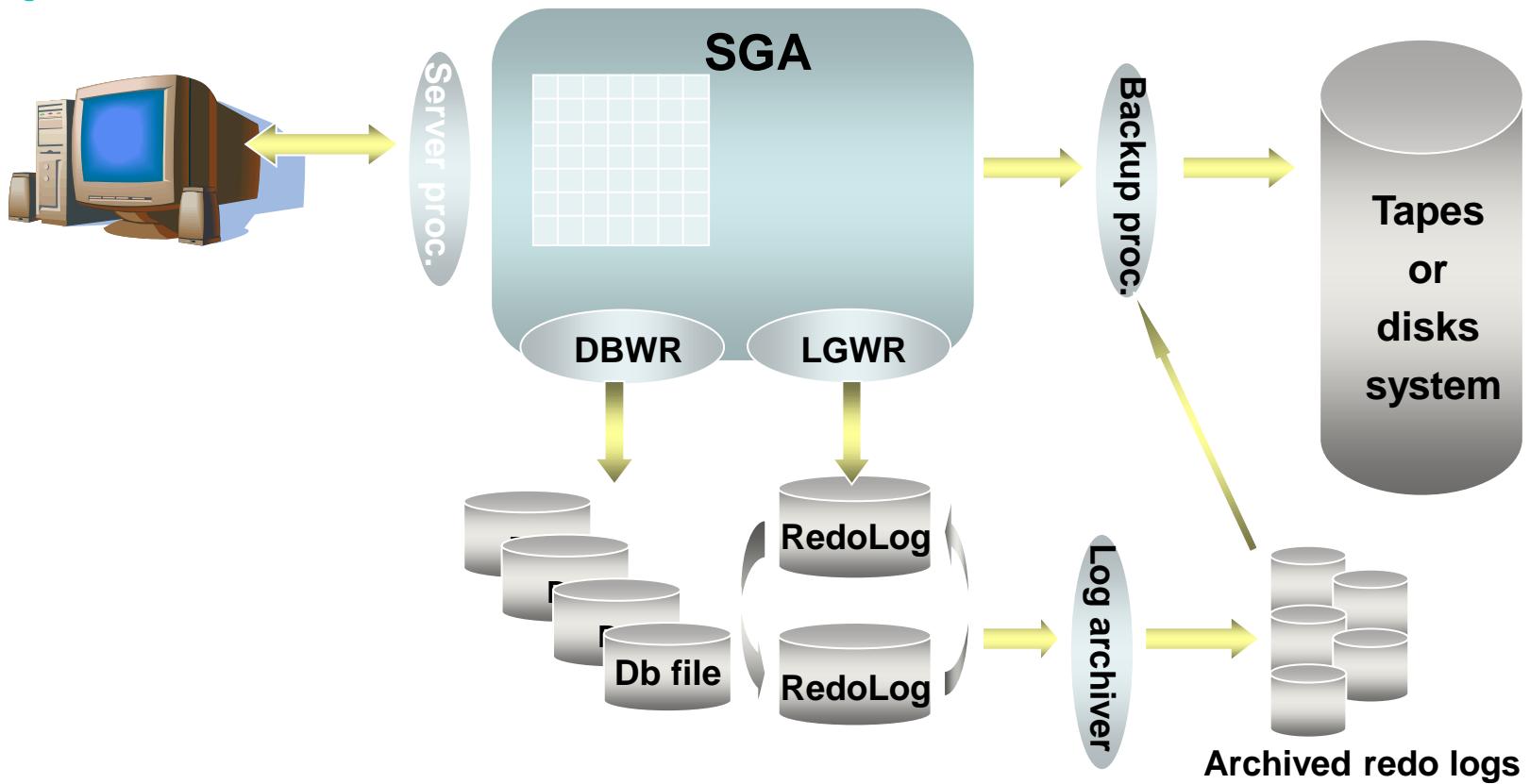
Backup options

- Physical backups
 - Cold (off-line) backups
 - Full database only
 - Require downtime
 - Do not provide flexibility for point in time recovery (PiTR)
 - Hot (on-line) backups
 - Different types of backups: full, incr. (cumulative, differential), archivelogs
 - Different scopes: full database, tablespace(s) or datafile(s)
 - Do not require database downtime
 - Can be used to recover full database, single/multiple tablespace(s)/datafile(s) or a corrupted block
 - Database can be recovered to any point in time within assumed backup retention period

Backup options

- Logical backups
 - Logical copy of data in the database
 - Support for different backup granularity
 - Can be taken either with legacy Export/Import tools or with Data Pump (10g)
- Standby systems (Data Guard)
 - Physical and logical standby databases

Como funciona un hot backup



¿Se puede solo
copiar y pegar
los archivos para
hacer backup?



Manual vs. RMAN backups

- RMAN advantages:
 - Supports incremental backup strategies
 - RMAN on-line backups are not so heavy for the system as manual on-line backups
 - RMAN can detect corrupted blocks
 - RMAN automatically track database structure changes
 - Provides easy, automated backup, restore and recovery operations
 - Keeps inventory of taken backups
 - Can seamlessly work with third party media managers
- Disadvantage: something new to learn
 - RMAN concepts and command syntax sometimes are not intuitive

VOLCADO DE DATOS

Database dump

- Contiene un registro de la estructura de la tabla y / o los datos de una base de datos y generalmente tiene la forma de una lista de instrucciones SQL . Un volcado de la base de datos se usa con mayor frecuencia para hacer una copia de seguridad de una base de datos para que su contenido se pueda restaurar en caso de pérdida de datos . Las bases de datos dañadas a menudo se pueden recuperar mediante el análisis del volcado.

Data PUMP

- Permite el movimiento rápido de datos y metadatos de una base de datos a otra.
- Está disponible desde el Oracle 10g
- Tiene utilidades de import y export

DATA PUMP

- Entre los parámetros mas utilizados está:

- INCLUDE/EXCLUDE
- DUMPFILE
- LOGFILE
- DIRECTORY
- COMPRESSION
- USERID
- CONTENT(ALL | DATA_ONLY | METADATA_ONLY)
- ESTIMATE_ONLY
- ESTIMATE= { BLOCKS | STATISTICS }
- QUERY

COMPRESSION={ALL | DATA_ONLY | METADATA_ONLY | NONE}

Métodos:

- FULL=Y
- SCHEMA=esquema1
- TABLES=[esquema.]tabla
- TABLESPACES=tbs01

Ejemplos

- expdp scott/tiger@db10g tables=EMP,DEPT directory=TEST_DIR dumpfile=EMP_DEPT.dmp logfile=expdpEMP_DEPT.log
- expdp scott/tiger@db10g schemas=SCOTT directory=TEST_DIR dumpfile=SCOTT.dmp logfile=expdpSCOTT.log
- expdp system/password@db10g full=Y directory=TEST_DIR dumpfile=DB10G.dmp logfile=expdpDB10G.log

Tutoriales impdp & expdp

- <https://www.adictosaltrabajo.com/2015/02/04/tutorial-impdp/>
- <https://www.adictosaltrabajo.com/2015/02/03/tutorial-expdp/>