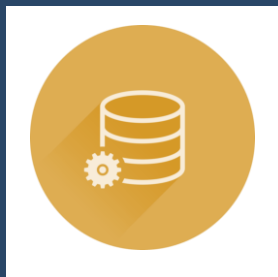


## II UNIDAD: MANTENIMIENTO DE BASE DE DATOS



### Tema: Planificación de los Respaldos y Restauración de Bases de Datos

Prof.: Pablo Argeñal

---

## DEFINICIONES BÁSICAS:



### RESPALDO / COPIA DE SEGURIDAD

Es la copia completa o parcial de una base de datos de un dispositivo primario en uno o varios dispositivos secundarios.

Los respaldos de una base de datos pueden ser físicos o lógicos.

Los términos copia de seguridad de datos y protección de datos a se encuentran vinculados estrechamente, dado que abarcan los objetivos más amplios de continuidad empresarial, seguridad de datos y administración del ciclo de vida de la información.

### RESTAURACIÓN

Es la recuperación de una base de datos de forma parcial o completa, la cual proviene de una copia de seguridad o respaldo. La restauración sobrescribe la información de la base de datos con la información de la copia de seguridad.

More info on how to use this template at  
[www.slidescarnival.com/help-use-presentation-template](http://www.slidescarnival.com/help-use-presentation-template)  
This template is free to use under [Creative Commons Attribution license](#).  
You can keep the Credits slide or mention SlidesCarnival and other resources used in a slide footer.



## PLAN DE MANTENIMIENTO DE BASES DE DATOS

---

### Plan de Administración de Copias de Seguridad

Consiste en la programación estratégica y sistematizada de la ejecución de las copias de seguridad de la base de datos, de los archivos lógicos y físicos de forma parcial o completa.

### Plan de Recuperación de Datos

Es el proceso de recuperación de bases de datos, que cubre la información parcial o total, dicha recuperación puede incluir el hardware y el software del SGBD, para que un negocio pueda comenzar de nuevo sus operaciones.

Confidencialidad

Seguridad  
de la información

Integridad

Disponibilidad



## SEGURIDAD INFORMÁTICA PLAN DE MANTENIMIENTO DE BASES DE DATOS

### SEGURIDAD INFORMÁTICA

La Seguridad Informática (S.I.) es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas, orientados a proveer condiciones seguras y confiables, para el procesamiento de datos en sistemas informáticos.

### CONTROLES DE SEGURIDAD

Son los mecanismos que se utilizan para poder administrar los accesos y privilegios a los recursos indicados. La implementación de controles de seguridad está regida por las políticas, normativas y procedimientos de seguridad.



**“La peor vulnerabilidad es la que se desconoce”**



### Amenaza:

Es una situación o acontecimiento que pueda causar daño a los bienes informáticos; puede ser una persona, un programa malicioso o un suceso natural o de otra índole y representan los posibles atacantes o factores que inciden negativamente sobre las debilidades del sistema.

### Riesgo:

Es la probabilidad de que una **amenaza** se materialice sobre una **vulnerabilidad** del sistema informático, causando un impacto negativo en la organización.

### Vulnerabilidad:

Es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.



## INFORMACIÓN A RESPALDAR Y FRECUENCIA

---

Un proceso de copia de seguridad se aplica a las bases de datos críticas o aplicaciones de línea de negocio relacionadas. El proceso se rige por políticas predefinidas de respaldo que especifican la frecuencia con la que se realiza la copia de seguridad de los datos y la cantidad de copias duplicadas (conocidas como réplicas), así como los acuerdos de nivel de servicio que estipulan la rapidez con la que se deben restaurar los datos.

# Best Practices



## INFORMACIÓN A RESPALDAR Y FRECUENCIA

---

Las mejores prácticas sugieren que se debe programar una copia de seguridad completa de los datos al menos una vez a la semana, a menudo durante los fines de semana o fuera del horario laboral. Para complementar las copias de seguridad completas semanales, las empresas generalmente programan una serie de tareas de respaldo de datos incrementales o diferenciales que solo realizan copias de los datos que han cambiado desde la última copia de seguridad completa.



# Best Practices



## MEDIOS DE ALMACENAMIENTO

---

Las empresas suelen realizar respaldo de datos clave en dispositivos de copia de seguridad dedicados o sistemas de cinta magnéticos. Los servidores de datos contienen unidades de disco duro (HDD) y están equipados con software para establecer políticas de respaldo.

Los sistemas de copia de seguridad de disco a disco aparecieron inicialmente como una alternativa a las bibliotecas de unidades de cinta de copia de seguridad magnética. Tanto el disco como la cinta todavía se usan hoy, y con frecuencia en conjunto.

<https://www.xataka.com/basics/hdd-vs-ssd>



## TIPOS DE COPIAS DE SEGURIDAD BD

---

### Copia completa

El método básico es el de copia completa o "Full copy" que realiza una copia directa de los archivos y directorios. Este proceso puede durar horas dependiendo del tamaño de los archivos o directorios a copiar, por lo que este proceso normalmente se ejecuta la primera vez o cada cierto tiempo.

Existen dos métodos más avanzados respecto a la copia completa que son la copia diferencial y la copia incremental. Dichas copias lo que realizan es un proceso de copia más avanzado permitiendo ahorrar tiempo, debido a que no se considera necesario realizar una copia completa cada día si no todos los archivos han sido modificados.



## TIPOS DE COPIAS DE SEGURIDAD BD

---

### Copia diferencial

La copia diferencial únicamente copia los archivos y directorios que han sido creados y/o modificados desde la última copia completa. Esto viene a suponer que si el lunes hemos realizado una copia completa y el martes ejecutamos una copia diferencial, únicamente se copiarán los ficheros creados o modificados durante el martes. Este mismo comportamiento se efectuará si la lanzamos el miércoles, tomando la copia completa del lunes como base.

Normalmente las copias diferenciales ocupan más espacio que las incrementales debido a que parten de la base de un único punto fijo en el tiempo ( la copia completa inicial ).



## TIPOS DE COPIAS DE SEGURIDAD BD

---

### Copia incremental

La copia incremental ( o diferencial incremental ) es la más avanzada al respecto, ya que únicamente copia los ficheros creados o modificados desde el último backup realizado, ya sea de una copia completa, diferencial o incremental, reduciendo de este modo los archivos a copiar y el tiempo empleado en el proceso de backup.

## TIPOS DE BACKUP

### SQL Server backup scenarios

This demonstrates Full, Differential and Transaction Log SQL server backup scenarios

#### 1. Full backup



For small databases with less important, read-only or easily-recoverable data

PROS: Easy to recover (just a single file), no database log needed (smaller database)

CONS: Can be recovered only up to the time of a backup, takes a lot of space

#### 2. Full + Differential backup



For big databases or databases with low transaction density where some data loss can be tolerated

PROS: Takes less space than full backup, no database log needed (smaller database), more precise restore

CONS: Can be recovered only up to the time of a backup, more complicated restore (needs two files)

#### 3. Full + Differential + Transaction log backup



For databases with high transaction density and/or important data where no data loss is tolerated

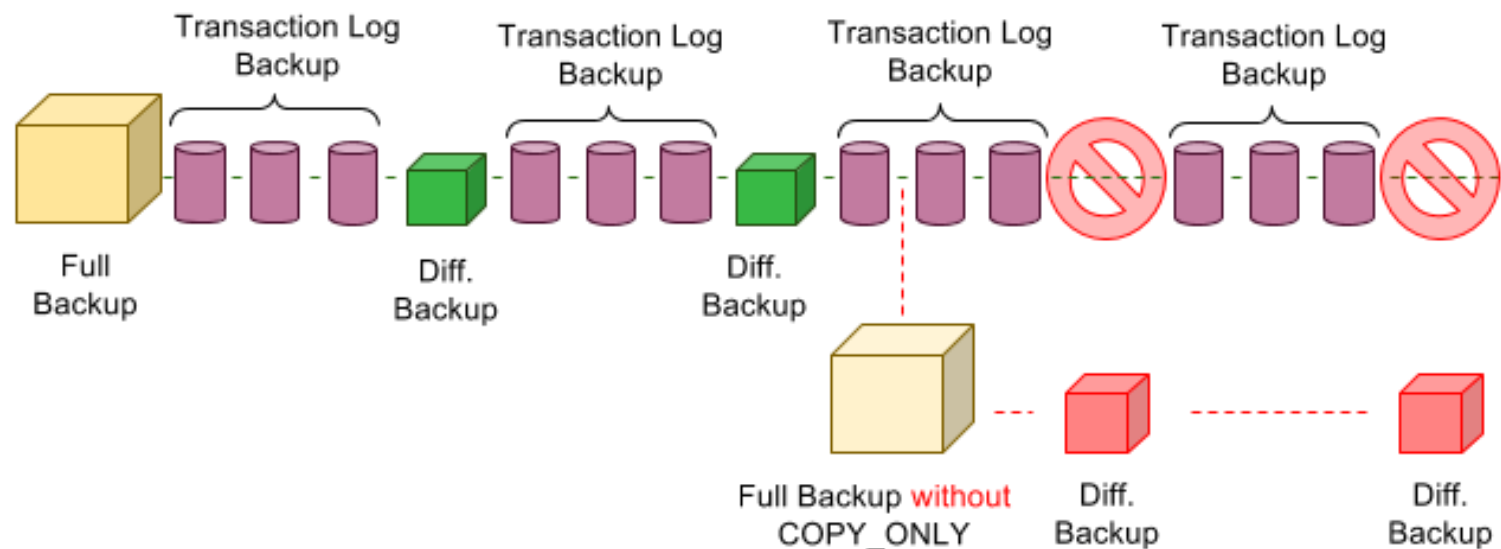
PROS: Database can be restored to any point of time with almost no data loss

CONS: A database needs transaction logging, larger in size, effortful restore process

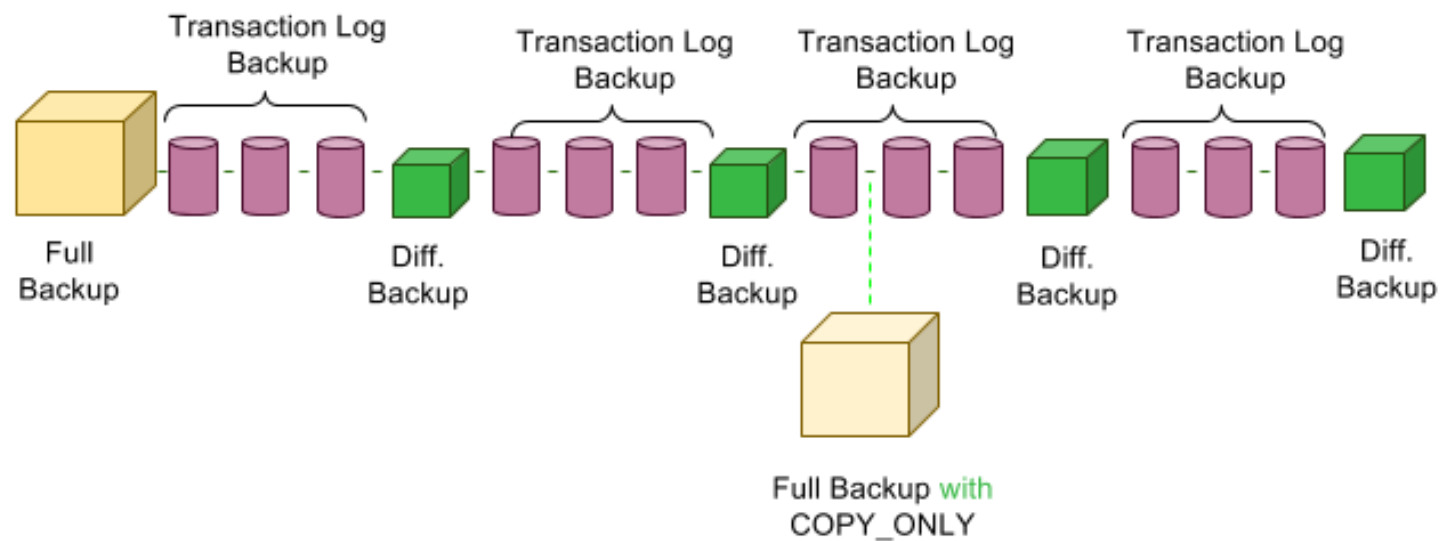
Requires SIMPLE recovery model

Requires FULL recovery model

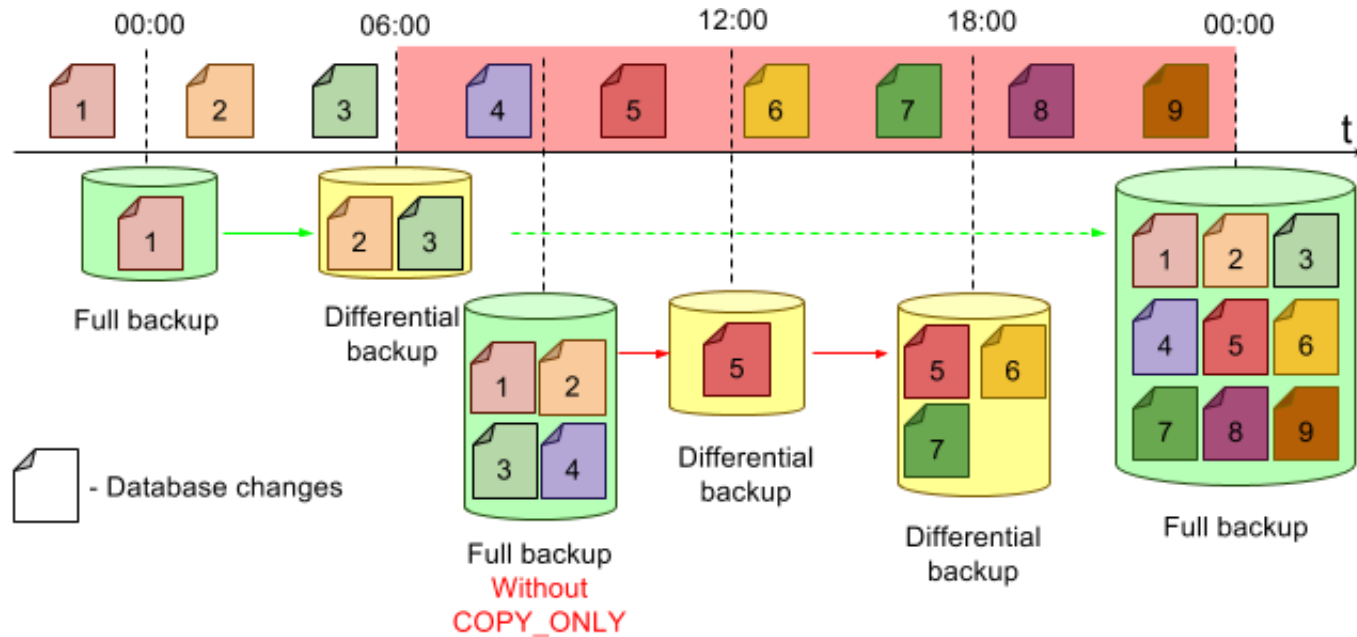
## LÓGICA DE EJECUCIÓN DE RESPALDOS



## LÓGICA DE EJECUCIÓN DE RESPALDOS

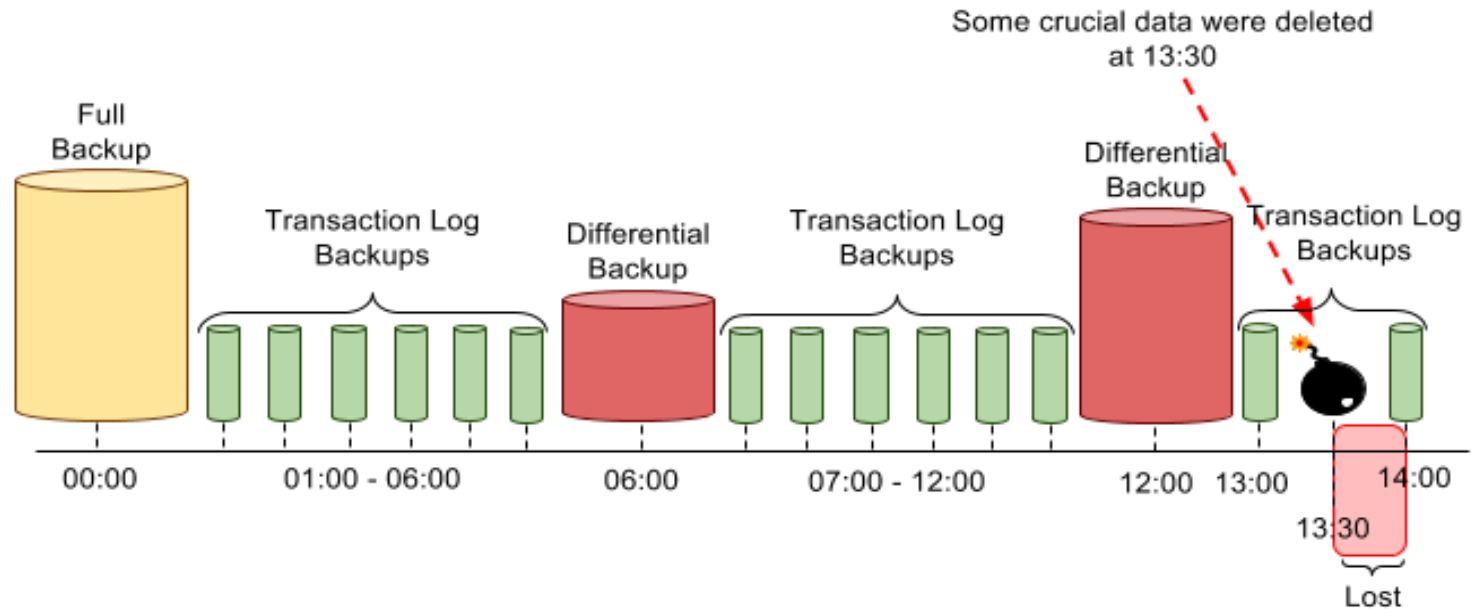


## LÓGICA DE EJECUCIÓN DE RESPALDOS





## LÓGICA DE EJECUCIÓN DE RESPALDOS





## PLANIFICACIÓN DE RESPALDOS

### TIPOS DE BASES DE DATOS

---

Todo proceso de planificación de respaldos debe ser revisado y aprobado por la alta dirección de la organización, se deberá establecer la mejor estrategia que permita el aseguramiento de la información tomando como referencia los siguientes parámetros:

- Tipo de Base de Datos: Dinámica o Estática
- Capacidad del Servidor
- Sensibilidad de los Datos

The image shows the back of a person with short, dark hair, wearing a light-colored sweater. They are standing in front of a wall covered in numerous sticky notes, some with diagrams and text. A semi-transparent blue overlay covers the entire image. The text "Gracias por su Atención" is centered in white.

**Gracias por su Atención**