

LABORATORIO FINAL - SOLUCIÓN

- 1) Liste los diferentes niveles de aislamiento que existen y describa un escenario en donde los aplicaría

1. Nivel: Aislamiento mínimo: Lectura no confirmada

Este nivel de aislamiento especifica que las instrucciones pueden leer filas que se modificaron por otros queries o transacciones previamente corridas pero que aún no se han confirmado. Aquí un ejemplo podría ser cuando se quiere aplicar un descuento, pero primero deben de leerse primero los datos de las filas, y luego ver si aplica o no el descuento.

2. Nivel: Aislamiento intermedio: Lectura confirmada

Este nivel de aislamiento se encarga de no dejar libres los datos que hayan sido modificados, pero no confirmados por otros queries o transacciones. Este nivel de aislamiento lo utilizaría para realizar un SP o un Trigger que este como al pendiente de cualquier cambio que se quiera realizar sobre los datos de la BD y que no puedan ni visualizarse y mucho menos modificarse por el o los usuarios en cuestión.

3. Nivel: Aislamiento intermedio: Lectura repetible

Este nivel de aislamiento propone que las instrucciones no puede leer datos que han sido modificados pero aún no confirmados por otras transacciones y que ninguna otra transacción puede modificar los datos leídos por la transacción actual hasta que haya finalizado. Un ejemplo en el que podríamos utilizar esto es para poder obtener vistas de datos actuales, entonces esto ayudaría a tener una idea de los datos confirmados que se tienen, pero sin opción a poder modificar o poder visualizar algún otro dato NO confirmado.

4. Nivel: Aislamiento máximo: Serializable

Aquí en definitiva podríamos utilizar este nivel de aislamiento para poder hacer carga de datos masivamente desde fuentes externas como lo que se realizó en el proyecto, desde un CSV, un txt, etc.

Transaction Isolation Level

		Isolation Level			
		Read Uncommitted	Read Committed	Repeatable Read	Serializable
Problem Type	Dirty Read	Possible	Not Possible	Not Possible	Not Possible
	Nonrepeatable Read	Possible	Possible	Not Possible	Not Possible
	Phantom Read	Possible	Possible	Possible	Not Possible

LABORATORIO FINAL - SOLUCIÓN

- 2) **Realizar** una consulta (query) que muestre la información de las ventas realizadas por cliente para los años entre 2011 y 2015, mostrando los datos como una tabla resumen:

	2011	2012	2013	2014	2015
CLIENTE 1	3756.989		5358.1451		
CLIENTE 2			2674.0227	650.8008	
CLIENTE 3	3756.989				

```
select p.FirstName as [Cliente], SUM(SOH.TotalDue) AS [Total Compra anual],  
YEAR(SOH.ModifiedDate) as [Año]  
from Sales.SalesOrderHeader SOH inner join Sales.Customer C on (SOH.CustomerID =  
C.CustomerID)  
inner join Person.Person p on P.BusinessEntityID = C.CustomerID  
group by C.PersonID , SOH.ModifiedDate, p.FirstName
```

- 3) **Enumere** los diferentes tipos de backup que pueden aplicarse y describa un escenario que considere vital por el cual debería de aplicar una política de respaldo en una empresa.
- Lógico**
Este tipo de respaldo lo podríamos aplicar para realizar un BackUp de una BD pequeña, que sea de interés personal para el propietario del manejador de BD
 - Físico**
Este tipo de BackUp se podría utilizar cuando queremos obtener el .mdb, y lo que queremos respaldar sean los diferentes datos pero en estado físico de nuestra BD
 - Completo**
Este tipo de BackUp lo podríamos utilizar cuando queremos tener un registro completo de toda la base de datos, desde el momento en que se creó hasta el día de hoy, por ejemplo, el historial o expediente de un alumno de un colegio.
 - Diferencial**
En este tipo de respaldo puede ser utilizado en beneficios de café donde se maneja la fermentación de café, ya que al momento de tener nuevos valores en las fermentaciones y tener configurada la base a realizar respaldos o Backups a cada hora se tendría únicamente los valores nuevos en los registros.

LABORATORIO FINAL - SOLUCIÓN

- 4) **Obtenga** un query para poder listar todos los objetos de la base de datos con sus respectivos privilegios que se han otorgado, como mínimo debería de tener la siguiente información:

OBJETO	ROL/USUARIO	PRIVILEGIO
Person.Person	AnalistaRH	Select

```
SELECT DISTINCT pr.default_schema_name,t.TABLE_NAME, pr.name, pe.permission_name
FROM sys.database_principals AS pr JOIN sys.database_permissions AS pe
ON pe.grantee_principal_id = pr.principal_id
JOIN [INFORMATION_SCHEMA].[TABLES] T ON pr.default_schema_name = t.TABLE_SCHEMA
```

- 5) Como encargado de la información de una Tienda de venta de artículos deportivos, por alguna razón, las personas de ventas, ingresan descuentos muy grandes en ciertos artículos. Solamente tienen permitido dar hasta un 25% de descuento sobre dichos artículos. El gerente te confirma que existen 2 aplicaciones para ingresar dicho descuento y que no es posible modificarlas en estos momentos. Qué puedes sugerir para asegurar que no existan descuentos mayores a 25% ¿?
- a. Crear una función que calcule dicho descuento.
 - b. Crear una *constraint* sobre la tabla de órdenes de venta.
 - c. Crear un trigger sobre la tabla de ordenes de venta que valide el descuento no mayor de 25% y hacer rollback si excede.
 - d. Crear una vista sobre las órdenes de venta que limite el descuento a 25%.
 - e. Dar permisos de lectura únicamente a la columna de descuento sobre el rol de ventas.
 - f. Ninguna de las anteriores.
 - g. Todas las anteriores

LABORATORIO FINAL - SOLUCIÓN

- 6) Como DBA, necesitas prevenir que los usuarios del departamento de Cuentas puedan modificar alguna data de la tabla de facturas, pero sí podrían visualizar dicha data. Todos estos usuarios, están asociados al rol de Cuentas, que tiene los permisos de SELECT, INSERT, UPDATE Y DELETE sobre dicha tabla de facturas.
- a. Se remueven todos los usuarios de dicho rol.
 - b. Ejecutar un “Deny”, para remover todos los privilegios de dichos usuarios.
 - c. Ejecutar “Grant” para incluir solo el permiso de SELECT para dichos usuarios.
 - d. Ejecutar “REVOKE” para remover todos los privilegios de dichos usuarios.