(AP1) → ACTIVIDAD PRÁCTICA 1

Responde las siguientes preguntas, de una forma concisa.

1. Busca en Internet las 10 bases de datos más grandes del mundo. Anota su nombre y tamaño.

BASE DE DATOS	TAMAÑO
World Data Center for Climate (WDCC)	140+ petabytes
Amazon Web Services (AWS)	100+ petabytes
Faceboock (Meta)	300+ petabytes
Google	15+ petabytes
Large HAdron Collider (LHC) - CERN	530+ petabytes
National Security Agency (NSA)	Calificado (Especula 1 yottabytes = 1 trillón de TB)
Youtube	1.000+ petabytes
Internet Archive	70+ petabytes
Spotify	100+ petabytes
Wayback Machine	70+ petabytes

2. Busca en Internet las leyes de CODD para el funcionamiento de SGBD relacionales y establece una relación entre cada una de las leyes de CODD y las funciones que proporcionan los SGBD actuales.

Regla 0: Un SGBD relacional debe gestionar sus BD de forma completa usando el modelo relacional

Regla 1: **Información**

- Todos los datos deben estar almacenados en tablas.
- Estas deben cumplir las premisas de modelo relacional.
- No puede haber información a la que accedamos por otra vía.

Regla 2: **Acceso garantizado**

- Cualquier dato es accesible sabiendo la clave de su fila y el nombre de su columna o atributo.
- Si un dato no podemos acceder de esta forma, no estamos usando un modelo relacional.

Regla 3: **Tratamiento sistemático de los valores nulos**

- Estos valores pueden dar significado a la columna que los contiene.
- El SGBD debe tener capacidad de manejar valores nulos.
- El SGBD reconocerá este valor como un valor distinto de cualquier otro.
- El SGBD sabrá aplicarle la lógica apropiada.
- Es un valor independiente del tipo de datos de la columna.

Regla 4: **Catalogo en línea relacional**

- El catálogo en línea es el diccionario de datos.
- El diccionario de datos se debe poder consultar usando las mistas técnicas que para los datos.
- Los metadatos, se organizan en tablas relacionales.
- Si SELECT es la instrucción que consulta datos, también será la que consulta los metadatos.

Regla 5: **Sublenguaje de datos completo**

- Tiene que existir, al menos, un lenguaje capaz de hacer todas las funciones del SGBD.
- No puede haber funciones fuera de ese lenguaje.
- Puede haber otros lenguajes en el SGBD para hacer ciertas tareas.
- Deben poder hacerse con el 'lenguaje completo'

Regla 6: **Vistas actualizadas**

- Las vistas tienen que mostrar información actualizada.
- No puede haber diferencia entre los datos de las vistas y los de las tablas base.

Regla 7: **Inserciones, modificaciones y eliminaciones de alto nivel**

- La idea es que el lenguaje que maneja la BD sea muy humano.
- Implica que las operaciones DML trabajen con conjuntos de filas a la vez.
- Para modificar, eliminar o añadir datos, no hará falta programar de la forma que lo hacen los lenguajes de 3ª generaciones (C o Java).

Regla 8: **Independencia física**

- ✓ Cambios en la física de la BD no afecta a las aplicaciones ni a los esquemas lógicos.
- ✓ El acceso a las tablas no cambia porque la física de la base de datos cambie.

Regla 9: **Independencia lógica**

- Cambios en el esquema lógico (tablas) no afectan al resto de esquemas.
- Si cambiamos nombres de tabla, o columna o modificamos información de las filas, las aplicaciones (esquema externo) no se ven afectadas.
- Es más difícil de conseguir.

Regla 10: **Independencia de integridad**

- Las reglas de integridad (restricciones) deben ser gestionadas y almacenadas por el SGBD.

Regla 11: **Independencia de distribución**

- Que la base de datos se almacene o gestione de forma distribuida en varios servidores, no afecta al uso de la misma ni a la programación de las aplicaciones de usuario.
- El esquema lógico es el mismo independientemente de si la BD es distribuida o no.

Regla 12: **No subversión**

- La BS no permitirá que exista un lenguaje o forma de acceso, que permita saltarse las reglas anteriores.

3. Busca el término SQL e indica las revisiones que ha sufrido el lenguaje a lo largo del tiempo.

Structured Query Lenguage. Es un lenguaje de consultas estructurado diseñado para interactuar con bases de datos relacionales. Tiene capacidad de hacer cálculos avanzados y algebra.

Es el estándar para gestionar y manipular los datos dentro de un SGBDR.

EVOLUCION	
1974 – 1975	Basado en el modelo relacional de Edgar Codd, IBM comienza a desarrollar un sistema de bases de datos, SEQUEL-XRM
	Se implementa el prototipo SEQUEL-XRM
1976 – 1977	Revisión del lenguaje, llamado SEQUEL/2
	Cambia nombre a SQL (razones legales)
	IBM adopta SQL en su prototipo de BD System R
1979	Relational Software, que luego se convierte en Oracle, lanza su propia versión comercial de SQL, Oracle V2.
1986 – 1987	ANSI publica el 1er estándar para SQL
	SQL se transforma en estándar internacional bajo ISO
1989	Estándar SQL es revisado, resultado en versión SQL/89, es una actualización menor del estándar original
1992	Se lanza SQL-92, versión mas robusta que introduce mejoras significativas (subconsultas, uniones externas…)
199 – 2000	Se introduce la versión SQL:1999, con consultas recursivas, soporte para objetos, y la estandarización de secuencias y columnas autonuméricas
	Algunas características de XML se incluyen en esta versión
2003	Microsoft lanza la versión SQL Server 2000 64 bit-Edition, compatible con Windows XP 64 bits y Windows Server
2005	El estándar ISO/IEC 9075-14:2005 define como SQL puede integrarse con XML. Importar, guardar y manipular datos XML dentro de una base de datos SQL, asi como el uso del lenguaje XQuery
2010	Se lanza SQL Server 2008 R2, con mejoras de escalabilidad, rendimiento y administración de BD para entornos críticos
2012	SQL Server 2012 mejora la confiabilidad para aplicaciones de misión crítica, con mejor rendimiento y seguridad.
2016	SQL Server 2016 incluye soporte para búsqueda de patrones, funciones de tabla polimórficas y compatibilidad con ficheros JSON.

4. Busca el término SQL Injection e indica por qué un administrador debe protegerse frente a él.

Es una técnica de ataque utilizada por los cibercriminales para explotar vulnerabilidades en las aplicaciones que interactúan con BD SQL. Permite al atacante ejecutar comandos SQL maliciosos en BD subyacentes a través de la entrada no validada de un usuario.

1. Acceso no autorizado a datos sensibles.
2. Modificación o eliminación de datos.
3. Compromiso del sistema.
4. Daños a la reputación.
5. Costos de remediación.
6. Cumplimiento normativo.