

1- Sentències preparades (o parametritzades)

a) Les sentències preparades SQL s'utilitzen per executar una mateixa sentència repetidament amb una gran eficiència.

b) Les sentències preparades permeten l'ús de paràmetres de substitució posicionals anònims amb el caràcter ?. Això ens permet que alguns dels valors de la sentència SQL no s'especifiquin, es canviïn per un ? i s'enviïn d'aquesta manera al servidor. Posteriorment, enviarem aquests valor des del client al servidor i així una mateixa sentència SQL es pot repetir moltes vegades amb valors diferents.

c) Les sentències preparades es realitzen en dues fases

1a - Preparació: Es prepara una platilla de la sentència SQL al servidor MySQL (prepare). Aquí és a on s'han d'utilitzar els paràmetres de substitució posicionals, utilitzant el caràcter ?. El servidor MySQL comprova que la sintaxi és correcta i inicialitza els seus recursos interns pel seu ús posterior.

2a - Execució: Es vincula (bind) cada paràmetre a un nou valor i s'envia els valors vinculats i l'ordre d'execució (execute) al servidor MySQL.

NOTA: Quan finalitzem l'ús de la sentència preparada, s'haurà de tancar per alliberar els recursos que utilitza.

d) Les sentències preparades ofereixen dos grans beneficis:

1- La sentència SQL només necessita ser preparada i analitzada un cop. La sentència SQL pot ser posteriorment executada múltiples vegades amb els mateixos o diferents valors. Com a resultat d'això, les sentències preparades usen menys recursos i s'executen més ràpidament.

2- Les sentències preparades separen les dades de la sentència i per aquest motiu es considera una tècnica adequada per insertar dades proporcionades i evitar per exemple [atacs d'injecció SQL](#).

d) No sempre és convenient utilitzar sentències preparades. Si només hem d'executar una sentència SQL, una sentència no preparada serà més eficient perquè es duent a terme menys comunicacions d'anada i tornada entre client i servidor.

2- Sentències preparades i ordres SQL DDL, DQL, DML i DCL

a) Llegeix com a recordatori: <https://www.geeksforgeeks.org/sql-ddl-dql-dml-dcl-tcl-commands/>

b) Recorda que les ordres SQL es divideixen en els següents 5 categories:

1. DDL – Data Definition Language → Exemples: CREATE, DROP, ALTER, TRUNCATE, COMMENT,..
2. DQL – Data Query Language → Exemple: SELECT
3. DML – Data Manipulation Language → Exemples: INSERT, UPDATE, DELETE
4. DCL – Data Control Language → Exemples: GRANT, REVOKE
5. TCL – Transaction Control Language → Exemples: COMMIT, ROLLBACK

c) En general, d'acord amb la documentació oficial de PHP, els paràmetres només són admesos dins de sentències de tipus DML i DQL. Trobareu més informació a la secció **Note** de la definició de **query** de l'apartat **parameters** de la següent pàgina documentació oficial de PHP: <https://www.php.net/manual/en/mysqli.prepare.php>. Tot i que parla de l'extensió MySQLi, aquesta nota també és vàlida per PDO.