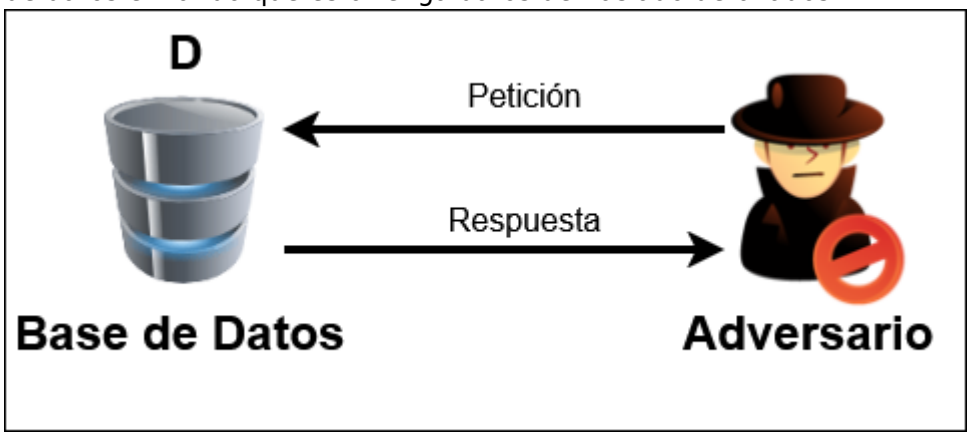
Ataques de reconstrucción de Bases de Datos

Un adversario quiere inferir algo de una base de datos mediante peticiones. Un ataque de inferencia está pensado para reconstruir una base de datos previamente curada. Se recomienda curar la base de datos evitando que esta tenga datos demasiado detallados.



Queremos proteger la base de datas contra el exceso de inferencias. El adversario puede tener una estrategia de peticiones dinámicas que van cambiando en fuinción a la información que van obteniendo. Para proteger los datos, se pueden denegar respuestas en función a lo peligrosas que puedan ser con respecto a la privacidad. El problema de denegar información es que a su vez puede dar información sin querer al adversario. Por ejemplo, si se pide el mayyor sueldo de un rango de empleados, sale X cifra, si luego hacemos la misma petición quitando un empleado y aparece una cifra diferente, podemos inferir el sueldo de dicho empleado.