1. **¿Qué aprendiste en cada sección del taller?**

* **Parte 1: Instalación y Configuración de MySQL**  
  Se aprendió a instalar MySQL en un sistema Windows y a configurarlo correctamente, como establecer una contraseña segura para el usuario root, configurar MySQL como un servicio para su inicio automático y ajustar los permisos en la carpeta de datos para mejorar la seguridad. Además, aprendí a verificar que MySQL se haya instalado correctamente ejecutando el comando SELECT VERSION();.
* **Parte 2: Creación de Base de Datos y Tablas**  
  Se aprendió a crear bases de datos y tablas dentro de MySQL. Creé una base de datos llamada seguridad\_mysql y luego una tabla usuarios que almacena información como el nombre, correo electrónico y contraseña encriptada de los usuarios.
* **Parte 3: Gestión de Usuarios y Privilegios**  
  Se aprendió a crear y gestionar usuarios en MySQL, asignando privilegios específicos sobre las bases de datos. Creé un usuario con permisos limitados y luego configuré los privilegios necesarios (SELECT, INSERT, UPDATE). También aprendí a revocar privilegios y eliminar usuarios cuando ya no son necesarios.
* **Parte 4: Seguridad en Bases de Datos**  
  Se aprendió a verificar y mejorar la seguridad en MySQL habilitando la autenticación segura, lo que garantiza que solo los usuarios con credenciales correctas puedan acceder. También configuré un firewall para bloquear accesos no deseados al puerto MySQL (3306), lo que añade una capa de seguridad adicional.
* **Parte 5: Manejo de Contraseñas y Encriptación**  
  Se aprendió a almacenar contraseñas de forma segura utilizando encriptación (SHA2). Esto ayuda a proteger las contraseñas de los usuarios al almacenarlas en un formato que no puede ser fácilmente revertido a texto plano.

1. **¿Qué dificultades encontraste y cómo las resolviste?**

* **Dificultad al configurar el firewall en Windows**: Durante la configuración del firewall de MySQL, encontré que los comandos PowerShell no siempre se ejecutaban correctamente debido a permisos insuficientes. Para resolverlo, aseguré que PowerShell se ejecutara con privilegios de administrador.
* **Manejo de la encriptación de contraseñas**: Aunque el proceso de encriptación con SHA2 fue sencillo, me costó entender cómo verificar si la contraseña estaba correctamente almacenada en la base de datos.

1. **¿Qué medidas de seguridad adicionales aplicarías en un entorno empresarial real?**

* **Uso de conexiones cifradas (SSL/TLS)**: Para proteger la transmisión de datos entre el cliente y el servidor MySQL, implementaría conexiones cifradas utilizando SSL/TLS. Esto aseguraría que los datos no puedan ser interceptados por atacantes durante su transmisión.