Evidencias

El alumno deberá entregar:

- Sentencias SQL completas y resultado obtenido
- Evidencia con consultas de verificación

Actividad 1 — Gestión de Usuarios y Roles (2 puntos)

1. Crea una base de datos llamada **sistema_ventas** y conéctate a ella.
2. Crea los siguientes usuarios:

Usuario	Requisitos
supervisor_ventas	Contraseña `Sup3r#2025`, puede crear roles, no puede crear BD, hereda privilegios
asistente_ventas	Contraseña `Asist$2025`, límite de 2 sesiones, no puede crear roles ni BD
inspector	Contraseña `Inspect#2025`, no hereda privilegios, solo 1 sesión

3. Crea un rol **ventas_equipo** con los siguientes requisitos:

- No inicia sesión
- Hereda permisos
- No crea BD ni roles
- No es superusuario
- No tiene permisos de replicación
- No puede omitir políticas

4. Asocia **supervisor_ventas** y **asistente_ventas** al rol **ventas_equipo**.
   El supervisor debe poder administrar permisos del rol; el asistente no.
5. Demuestra la pertenencia a los roles con consultas.
6. Con el usuario ***asistente*_ventas**, crea una tabla llamada **productos** y luego intenta eliminar el usuario desde otro perfil.

    - ¿Qué sucede y por qué?
    - ¿Qué pasos serían necesarios para eliminarlo correctamente?
    - ¿Qué riesgos implicaría forzar su eliminación?

Actividad 2 — Vistas y Accesos Controlados (2 puntos)

1. Crea las tablas e inserta datos:

clientes(id, nombre, telefono, email, saldo, vip boolean)
ventas(id, id_cliente, fecha, total, estado)

2. Inserta al menos 3 clientes y 3 ventas de ejemplo.
3. Crea las siguientes vistas:

Vista	Contenido	Quién accede
vista_admin_clientes	Todos los datos + suma total gastado por cliente	supervisor_ventas
vista_asistente_clientes	Nombre, teléfono, saldo, vip (sin email)	asistente_ventas
vista_inspector_anonima	Solo totales por cliente sin información personal	inspector

4. Revoca permisos directos sobre las tablas base a todos los usuarios excepto el superusuario.
   Concede permisos solamente a través de vistas.
5. Demuestra las diferencias al consultar con cada usuario.

Actividad 3 — Auditoría, Seguridad y Políticas (2 puntos)

1. Crea un rol adicional llamado **solo_lectura_global** y:

- Dale acceso de *solo lectura* a todas las tablas y vistas existentes.
- Haz que el usuario inspector herede este rol.
- Asegura que cualquier objeto futuro creado en el esquema sea accesible en lectura por este rol.

Actividad 4 — Práctica de Revocación y Cambios de Privilegios (2 puntos)

1. Sobre la tabla clientes:

- Concede a **ventas_equipo** permisos de INSERT y SELECT.
- Concede a **supervisor_ventas** permiso de DELETE.
- Revoca explícitamente DELETE a **asistente_ventas**.

2. Luego:

- Revoca TODOS los permisos del rol ventas_equipo sobre clientes.
- Vuelve a conceder solo SELECT.

Actividad 5 — Informe de Seguridad (2 puntos)

1. Modifica autenticación en `pg_hba.conf` para usar **scram-sha-256**.
   Activa el log y registra intentos de conexión fallidos.

Entrega:

- Captura de logs con fallos
- Verifica los privilegios de cada usuario