

# ACTIVIDAD 5 – SEGURIDAD Y CUMPLIMIENTO

Cristóbal Suárez Abad

ADMINISTRACIÓN DE SISTEMAS GESTORES DE BASES DE DATOS - 2º ASIR

## Contenido

|  |          |
|--|----------|
| <b>Actividad 5 – Seguridad y cumplimiento.....</b>   | <b>2</b> |
| <b>Configuración de políticas de seguridad .....</b> | <b>2</b> |
| <b>Auditoría de accesos.....</b>                     | <b>4</b> |
| <b>Comprobación de seguridad.....</b>                | <b>6</b> |



- Cambia la política de autenticación de `md5` a `scram-sha-256` en `pg_hba.conf`.

```
# IPv4 local connections:
host    all             all             127.0.0.1/32         scram-sha-256
host    all             securisimo      0.0.0.0/0            scram-sha-256
# IPv6 local connections:
host    all             all             ::1/128             scram-sha-256
# Allow replication connections from localhost, by a user with the
# replication privilege.
local   replication      all                                     peer
host    replication      all             127.0.0.1/32         scram-sha-256
host    replication      all             ::1/128             scram-sha-256
host    all              all             0.0.0.0/0            scram-sha-256
```

## Auditoría de accesos

- Conéctate con distintos usuarios y revisa los logs.

Para saber dónde están los logs:

Te metes en **postgresql**:

Encuentra el Directorio de Datos (PGDATA): **SHOW data\_directory;**

Verifica el Directorio de Logs: **SHOW log\_directory;**

Determina el Nombre del Archivo de Log Actual (si el servidor está en ejecución):

**SELECT pg\_current\_logfile();**

```
postgres=# SHOW data_directory;
 data_directory
-----
/var/lib/postgresql/16/main
(1 row)

postgres=# SHOW log_directory;
 log_directory
-----
log
(1 row)

postgres=# SELECT pg_current_logfile();
 pg_current_logfile
-----
log/postgresql-2025-11-14_095314.log
(1 row)
```

En “/var/lib/postgresql/16/main/log/”:

“Logeo” **exitoso**:

```
2025-11-14 10:04:38.615 CET [2748] [unknown]@[unknown] LOG: connection received: host=172.16.40.105 port=63714
2025-11-14 10:04:38.632 CET [2748] auditor@ventas_db LOG: connection authenticated: identity="auditor" method=scram-sha-256 (/etc/postgresql/16/main/pg_hba.conf:150)
2025-11-14 10:04:38.632 CET [2748] auditor@ventas_db LOG: connection authorized: user=auditor database=ventas_db SSL enabled (protocol=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384, bits=256)
2025-11-14 10:04:38.655 CET [2749] [unknown]@[unknown] LOG: connection received: host=172.16.40.105 port=63715
2025-11-14 10:04:38.672 CET [2749] auditor@ventas_db LOG: connection authenticated: identity="auditor" method=scram-sha-256 (/etc/postgresql/16/main/pg_hba.conf:150)
2025-11-14 10:04:38.672 CET [2749] auditor@ventas_db LOG: connection authorized: user=auditor database=ventas_db SSL enabled (protocol=TLSv1.3, cipher=TLS_AES_256_GCM_SHA384, bits=256)
2025-11-14 10:04:42.530 CET [2750] [unknown]@[unknown] LOG: connection received: host=172.16.40.105 port=63718
```

- o Identifica intentos fallidos de conexión. Explica que ves

“Logeo” **fallido**:

```
2025-11-14 10:07:42.661 CET [2829] perro_sanchez@ventas_db DETAIL: Role "perro_sanchez" does not exist.
Connection matched file "/etc/postgresql/16/main/pg_hba.conf" line 150: "host all all 0.0.0.0/0 scram-sha-256"
2025-11-14 10:07:44.899 CET [2830] [unknown]@[unknown] LOG: connection received: host=172.16.40.105 port=63765
2025-11-14 10:07:44.916 CET [2830] perro_sanchez@ventas_db FATAL: password authentication failed for user "perro_sanchez"
2025-11-14 10:07:44.916 CET [2830] perro_sanchez@ventas_db DETAIL: Role "perro_sanchez" does not exist.
Connection matched file "/etc/postgresql/16/main/pg_hba.conf" line 150: "host all all 0.0.0.0/0 scram-sha-256"
2025-11-14 10:07:46.558 CET [2832] [unknown]@[unknown] LOG: connection received: host=172.16.40.105 port=63766
2025-11-14 10:07:46.575 CET [2832] perro_sanchez@ventas_db FATAL: password authentication failed for user "perro_sanchez"
2025-11-14 10:07:46.575 CET [2832] perro_sanchez@ventas_db DETAIL: Role "perro_sanchez" does not exist.
Connection matched file "/etc/postgresql/16/main/pg_hba.conf" line 150: "host all all 0.0.0.0/0 scram-sha-256"
```

Me indica hora, IP y nombre del usuario que intenta conectarse, también la conexión configurada en “pg\_hba.conf” que se le aplicaría.

## Comprobación de seguridad

- o Verifica los privilegios de cada usuario (`\du` y `\z`).

```
postgres=# \du
```

| Role name       | Attributes  |
|-----------------|---|
| admin_ventas    | Create role, Create DB +<br>Password valid until 2026-12-31 00:00:00+01 |
| auditor         | No inheritance +<br>15 connections                                      |
| cristobal       |   |
| empleado_ventas | 3 connections   |
| postgres        | Superuser, Create role, Create DB, Replication, Bypass RLS              |
| segurísimo      | Superuser, Create role, Create DB, Replication, Bypass RLS              |
| solo_lectura    | Cannot login  |
| ventas_acceso   | 10 connections  |
| ventas_grupo    | Cannot login  |

```
postgres=# \z
```

| Schema | Name            | Type          | Access privileges         | Column privileges | Policies |
|--------|-----------------|---------------|---------------------------|-------------------|----------|
| public | clientes        | table         |                           |                   |          |
| public | clientes_id_seq | sequence      |                           |                   |          |
| public | pedidos         | table         |                           |                   |          |
| public | pedidos_id_seq  | sequence      |                           |                   |          |
| public | productos       | foreign table | postgres=arwdDxt/postgres |                   |          |

(5 rows)

- Elabora un informe final indicando qué medidas garantizan la seguridad.
- **Vistas personalizadas:** Cada usuario solo accede a las columnas y datos esenciales para su función, ocultando información sensible (DNI, Email).
- **Revocación de Permisos Directos:** Se fuerza a los usuarios a usar las vistas, asegurando que las políticas de filtrado y exposición de datos se cumplan.
- **Restricción de Conexiones:** Previene el abuso o el uso excesivo de recursos por parte de cuentas individuales.
- **Asignación de Permisos de Manipulación Detallada:** Solo admin\_ventas tiene el poder de eliminar registros, mientras que empleado\_ventas solo puede insertar/actualizar.
- **Rol solo\_lectura:** Centraliza y simplifica la concesión de acceso de solo lectura para la auditoría.
- **Autenticación scram-sha-256:** Mejora la seguridad de las contraseñas almacenadas, haciéndolas menos susceptibles a ataques que la política md5.
- **Registro de Actividad:** Permite detectar y rastrear intentos fallidos, accesos no autorizados y actividades sospechosas, garantizando el cumplimiento.