# Configuración de la Base de Datos

**Sistema de Gestión Bancaria y Antifraude**

**Autor:** Joaquín Manuel Alpañez López  
**Rol Profesional:** Consultor Técnico Especializado en Banca  
**Fecha de Creación:** 21 de octubre de 2025  
**Última Modificación:** 21 de octubre de 2025  
**Versión de Oracle Database:** Oracle 12c Express Edition  
**Entorno de Desarrollo:** Oracle SQL Developer 24.3.1

## 1. Propósito del Documento

El presente documento describe la configuración inicial de la base de datos utilizada en el proyecto de creacion de un sistema de gestión bancaria y antifraude. Este script constituye la base estructural para la creación de un entorno de desarrollo controlado, estable y seguro, orientado a la gestión bancaria, auditorías y procesos antifraude. Se detalla la creación de los tablespaces, roles, usuarios, políticas de auditoría y parámetros de seguridad del sistema.

## 2. Alcance

Este script se ha diseñado para entornos de desarrollo y pruebas. Su propósito es establecer una estructura de base sólida que simula las condiciones de un entorno bancario profesional, incluyendo políticas de seguridad, auditoría y control de acceso. No se recomienda su uso directo en entornos productivos sin adaptación previa por parte de un DBA.

## 3. Estructura General del Script

El script está compuesto por diversos bloques funcionales, cada uno con un objetivo claro dentro de la configuración general del entorno de base de datos. A continuación se describen las secciones principales:

### 3.1 Bloque de Ejecución y Trazabilidad

Define las condiciones de ejecución del script, incluyendo el usuario con rol SYSDBA, el contenedor PDB a utilizar y los parámetros de sesión requeridos. Se activan las auditorías, trazas SQL y el estado persistente de la base de datos.

### 3.2 Configuración de Tablespaces

Crea los tablespaces principales (DATA\_TBS e INDEX\_TBS) que gestionarán los datos y los índices del sistema. Estos se configuran con crecimiento automático (AUTOEXTEND) y asignación automática de segmentos.

### 3.3 Configuración de Roles

Define los roles de seguridad que controlan los niveles de acceso y permisos. Incluye roles de administración, auditoría, reporting y operaciones comunes. Se aplican privilegios de sistema según el propósito del rol.

### 3.4 Configuración de Usuarios

Crea los usuarios funcionales y técnicos del sistema (USR\_CFG, USR\_BACKEND, USR\_REPORTING, USR\_ADMIN, etc.) y asigna a cada uno su rol correspondiente, tablespace predeterminado y cuota de almacenamiento.

### 3.5 Configuración de Auditoría

Establece políticas de auditoría para registrar eventos críticos como inicios de sesión, creación o eliminación de objetos, modificaciones de usuarios y concesión de privilegios.

### 3.6 Configuración de Seguridad y Políticas de Contraseñas

Aplica restricciones y reglas sobre las contraseñas, incluyendo tiempo de vida, intentos fallidos, verificación de complejidad y políticas de reutilización.

### 3.7 Consultas de Verificación Posterior

Incluye sentencias SELECT que permiten verificar la correcta creación de usuarios, roles, privilegios y auditorías tras la ejecución del script.

## 4. Notas Técnicas y Consideraciones

- Los parámetros de auditoría y las configuraciones de sistema son permanentes una vez aplicados.  
- El comando 'ALTER PLUGGABLE DATABASE SAVE STATE' guarda el estado del contenedor para futuras aperturas automáticas.  
- 'ALTER SYSTEM SET AUDIT\_TRAIL = DB, EXTENDED SCOPE = SPFILE' requiere reinicio del servicio de base de datos.  
- Se recomienda no ejecutar los bloques de borrado (DROP) fuera de entornos de prueba.  
- La configuración de perfiles de contraseñas afecta a todos los usuarios asociados al perfil DEFAULT.

## 5. Recomendaciones para Entornos Profesionales

Para un entorno corporativo, se recomienda:  
- Asignar tablespaces dedicados por esquema o aplicación.  
- Implementar políticas de auditoría más granulares (por esquema o tipo de evento).  
- Desactivar 'AUTOEXTEND' y controlar manualmente el crecimiento de los datafiles.  
- Configurar políticas de contraseñas personalizadas por rol o tipo de usuario.  
- Implementar backups automáticos mediante RMAN o herramientas equivalentes.

## 6. Conclusión

Este script establece una base técnica sólida para el entorno de desarrollo del Sistema de Gestión Bancaria y Antifraude. Garantiza la seguridad, la trazabilidad y la organización de los objetos de base de datos desde las primeras fases del proyecto.