ESTRATEGIA DE CIBERSEGURIDAD ENTERPRISE & GOBIERNO DE DATOS

Plan de Migración Privilegiada y Seguridad MS SQL Server 2022

PLATAFORMA:	NORMATIVAS:	ARTEFACTO:	DOCUMENTO ID:
SQL Server 2022	ISO 27001 / 27018	[dba].[UserManagement]	SEC-SQL-2026-v3

1. RESUMEN EJECUTIVO Y ALCANCE

El presente plan documenta el proceso estándar para erradicar el uso de la cuenta superadministradora predefinida `sa` en entornos Microsoft SQL Server 2022. La solución se sustenta en un modelo **Role-Based Access Control (RBAC)** administrado centralizadamente mediante el procedimiento almacenado Enterprise `[dba].[UserManagement]`.

CONTROLES ENTERPRISE INTEGRADOS

El procedimiento almacenado incluye 6 capacidades avanzadas: **Pre-flight Checks** en `msdb`, **Snapshot JSON de Permisos con capacidad de Rollback**, **Reparación de Usuarios Huérfanos**, **Reporte RBAC en Pantalla**, **Verificación de Ownership Chaining** y **Blindaje del Esquema de Auditoría [AUD]**.

2. ESTRATEGIA DE REEMPLAZO Y DESACTIVACIÓN DE SA

La desactivación de la cuenta `sa` se efectúa bajo el siguiente flujo seguro sin interrupción de servicio:

FASE	ACCIÓN TÁCTICA	GARANTÍA DE SEGURIDAD / CONTROL ISO
1. Pre-Check	Validar Jobs de Agent y DB Owner (PRE_CHECK).	A.8.15 - Evita la caída de tareas automáticas al detectar dependencias de `sa`.
2. Sysadmin Alt.	Crear administradores nominativos.	A.5.17 - Identificación y responsabilidad individual en cuentas de privilegio.
3. Re-owner Jobs	Asignar Jobs de Agent al nuevo sysadmin.	A.8.2 - Garantiza que ningún job activo pertenezca a la cuenta que se va a desactivar.
4. Desactivación	Ejecutar `ALTER LOGIN [sa] DISABLE`.	A.5.15 - Bloquea la superficie de ataque sobre el SID fijo de la cuenta SA.

3. MATRIZ DE ROLES Y PERFILES DE TRANSICIÓN

Los accesos a las bases de datos se otorgan exclusivamente a través de los siguientes Roles:

- `dba_users`: Control total sobre esquemas administrados (`GRANT CONTROL ON SCHEMA`).
- `app_users`: Perfil para aplicaciones web/APIs con dos niveles de madurez:
  - `HYBRID`: Otorga `SELECT`, `INSERT`, `UPDATE` y `EXECUTE`. Deniega `DELETE` y DDL (`ALTER`).
  - `SP_ONLY`: Cancela el acceso inline y habilita exclusivamente `EXECUTE` sobre Stored Procedures.
- `bistats_users`: Acceso de solo lectura (`GRANT SELECT`) para inteligencia de negocios y reportes.
- `dev_users`: Lectura, escritura y ejecución para entornos de prueba, denegando alteración estructural (`DENY ALTER`).

4. PROCEDIMIENTO ALMACENADO [DBA].[USERMANAGEMENT]

A continuación se incluye el código T-SQL del procedimiento centralizado con soporte de auditoría JSON:

```
USE [master];
GO
IF NOT EXISTS (SELECT * FROM sys.schemas WHERE name = 'dba') EXEC('CREATE SCHEMA [dba]');
IF NOT EXISTS (SELECT * FROM sys.schemas WHERE name = 'AUD') EXEC('CREATE SCHEMA [AUD]');
GO

CREATE OR ALTER PROCEDURE [dba].[UserManagement]
    @OperationType VARCHAR(50),       -- 'PRE_CHECK', 'DISABLE_SA', 'CREATE_SYSADMIN', 'ASSIGN_ROLE_USER',
'AUDIT_REPORT', 'FIX_ORPHAN'
    @LoginName SYSNAME = NULL,        -- Login de SQL Server
    @Password NVARCHAR(128) = NULL,   -- Contraseña (necesaria para nuevos logins)
    @TargetDatabase SYSNAME = 'master',-- Base de datos objetivo
    @RoleName SYSNAME = NULL,         -- 'dba_users', 'app_users', 'bistats_users', 'dev_users'
    @TargetSchema SYSNAME = 'dbo',    -- Esquema al que se aplica la regla
    @AppProfile VARCHAR(20) = 'HYBRID'-- Para app_users: 'HYBRID' o 'SP_ONLY'
AS
BEGIN
    SET NOCOUNT ON;
    DECLARE @SPID INT = @@SPID, @SystemUser SYSNAME = SYSTEM_USER, @OriginalLogin SYSNAME =
ORIGINAL_LOGIN();
    DECLARE @HostName SYSNAME = HOST_NAME(), @AppName NVARCHAR(128) = APP_NAME();
    DECLARE @SQL NVARCHAR(MAX), @Message NVARCHAR(MAX), @Severity TINYINT = 1, @SnapshotJSON NVARCHAR(MAX)
= NULL;

    BEGIN TRY
        -- PRE-FLIGHT CHECKS
        IF @OperationType = 'PRE_CHECK'
        BEGIN
            SET @Message = CONCAT('Pre-Flight Checks en servidor: ', @@SERVERNAME);
            SELECT j.job_id, j.name AS [JobName], s.name AS [OwnerName], j.enabled FROM msdb.dbo.sysjobs j
JOIN sys.server_principals s ON j.owner_sid = s.sid WHERE s.name = 'sa';
            SELECT name AS [DatabaseName], SUSER_SNAME(owner_sid) AS [DatabaseOwner] FROM sys.databases
WHERE SUSER_SNAME(owner_sid) = 'sa';
        END

        -- REPARACIÓN DE HUÉRFANOS
        ELSE IF @OperationType = 'FIX_ORPHAN'
        BEGIN
            SET @SQL = N'USE ' + QUOTENAME(@TargetDatabase) + N'; ALTER USER ' + QUOTENAME(@LoginName) +
N' WITH LOGIN = ' + QUOTENAME(@LoginName) + N';';
            EXEC sp_executesql @SQL;
            SET @Message = CONCAT('Usuario huérfano ', @LoginName, ' reconectado en DB ',
@TargetDatabase);
        END

        -- DESACTIVACIÓN DE SA
        ELSE IF @OperationType = 'DISABLE_SA'
        BEGIN
            IF EXISTS (SELECT 1 FROM msdb.dbo.sysjobs j JOIN sys.server_principals s ON j.owner_sid =
s.sid WHERE s.name = 'sa' AND j.enabled = 1)
                RAISERROR('Existen Jobs activos de SQL Server Agent cuya propiedad es de SA. Reasigne los
jobs antes de desactivar SA.', 16, 1);

            ALTER LOGIN [sa] DISABLE;
            SET @Message = 'La cuenta superadministradora predefinida [sa] ha sido DESACTIVADA.';
        END

        -- CREACIÓN DE SYSADMIN
        ELSE IF @OperationType = 'CREATE_SYSADMIN'
        BEGIN
            IF NOT EXISTS (SELECT 1 FROM sys.server_principals WHERE name = @LoginName)
            BEGIN
                SET @SQL = N'CREATE LOGIN ' + QUOTENAME(@LoginName) + N' WITH PASSWORD = ' +
QUOTENAME(@Password, '''') + N', CHECK_POLICY = ON;';
                EXEC sp_executesql @SQL;
            END
            SET @SQL = N'ALTER SERVER ROLE [sysadmin] ADD MEMBER ' + QUOTENAME(@LoginName) + N';';
            EXEC sp_executesql @SQL;
            SET @Message = CONCAT('Sysadmin creado y asignado: ', @LoginName);
        END
```

5. GUÍA DE EJECUCIÓN OPERATIVA

Fase 1: Pre-Check y Desactivación de SA

```
-- 1. Verificar dependencias de Jobs antes de desactivar SA
EXEC [dba].[UserManagement] @OperationType = 'PRE_CHECK';

-- 2. Crear el administrador nominativo de reemplazo
EXEC [dba].[UserManagement]
    @OperationType = 'CREATE_SYSADMIN',
    @LoginName = 'admin_sys_main',
    @Password = 'C0mpl3x#P@ss2026!Key',
    @TargetDatabase = 'master';

-- 3. Desactivar SA de forma segura
EXEC [dba].[UserManagement] @OperationType = 'DISABLE_SA';
```

Fase 2: Configuración de Aplicación (Perfil Híbrido y SP-Only)

```
-- Configuración Híbrida Transicional (Sin DELETE/ALTER inline)
EXEC [dba].[UserManagement]
    @OperationType = 'ASSIGN_ROLE_USER',
    @LoginName = 'appuser',
    @Password = 'AppSecure#Pass2026',
    @TargetDatabase = 'ProduccionDB',
    @RoleName = 'app_users',
    @TargetSchema = 'dbo',
    @AppProfile = 'HYBRID';

-- Cierre Final de Grifo (Solo Stored Procedures)
EXEC [dba].[UserManagement]
    @OperationType = 'ASSIGN_ROLE_USER',
    @LoginName = 'appuser',
    @TargetDatabase = 'ProduccionDB',
    @RoleName = 'app_users',
    @TargetSchema = 'dbo',
    @AppProfile = 'SP_ONLY';
```

Fase 3: Reparación de Huérfanos y Auditoría en Pantalla

```
-- Vincular usuario huérfano a su login tras una restauración
EXEC [dba].[UserManagement]
    @OperationType = 'FIX_ORPHAN',
    @LoginName = 'appuser',
    @TargetDatabase = 'ProduccionDB';

-- Proyectar la matriz RBAC en pantalla para auditoría
EXEC [dba].[UserManagement]
    @OperationType = 'AUDIT_REPORT',
    @TargetDatabase = 'ProduccionDB';
```

6. MATRIZ DE CUMPLIMIENTO ISO/IEC 27001 Y 27018

CONTROL NORMATIVO	REQUISITO DEL ESTÁNDAR	MECANISMO TÉCNICO EN [DBA].[USERMANAGEMENT]
ISO 27001 - A.5.15 *Access Control*	Restringir accesos al principio de menor privilegio.	Asignación de roles por esquema con opción de restricción absoluta a Stored Procedures (`SP_ONLY`).
ISO 27001 - A.5.17 *Authentication Info*	Gestión segura de identidades de privilegio.	Desactivación total de `sa` previo control de dependencias con `PRE_CHECK`.
ISO 27001 - A.8.15 *Logging & Monitoring*	Registro y auditoría de eventos administrativos.	Inclusión de **Snapshot JSON** con historial previo de permisos en la tabla `[AUD].[AuditLog]`.
ISO 27001 - A.8.2 *Privileged Access*	Limitación y control de privilegios especiales.	Sustitución de privilegios globales de servidor por roles acotados a esquemas específicos.