

Universidad Peruana Los Andes
Facultad de Ingeniería
Escuela profesional de Ingeniería de Sistemas



Curso: Base de datos II
Docente: Raul Enrique Fernandez Bejarano
Estudiante: Sarmiento Mosquera Yeims Abraham
Ciclo: V - Código: s03807f

Huancayo - 2025

1. Autenticación SQL y Windows: diferencias y prácticas seguras

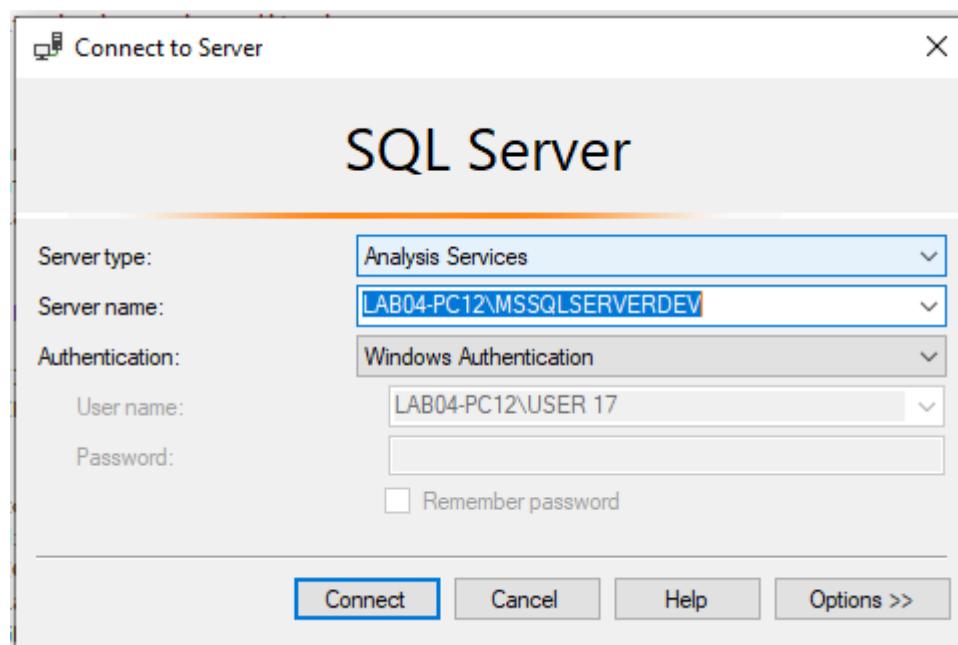
Diferencias:

Autenticación de Windows	Autenticación de SQL
<ul style="list-style-type: none">• Usa las credenciales del sistema operativo.	<ul style="list-style-type: none">• Requiere usuario y contraseña definidos en SQL Server.
<ul style="list-style-type: none">• Más segura porque integra políticas de dominio, contraseñas y auditoría.	<ul style="list-style-type: none">• Útil cuando no se puede usar Active Directory (por ejemplo, en entornos aislados).
<ul style="list-style-type: none">• Ideal para entornos corporativos con Active Directory.	<ul style="list-style-type: none">• Debe configurarse con contraseñas fuertes y políticas de expiración.

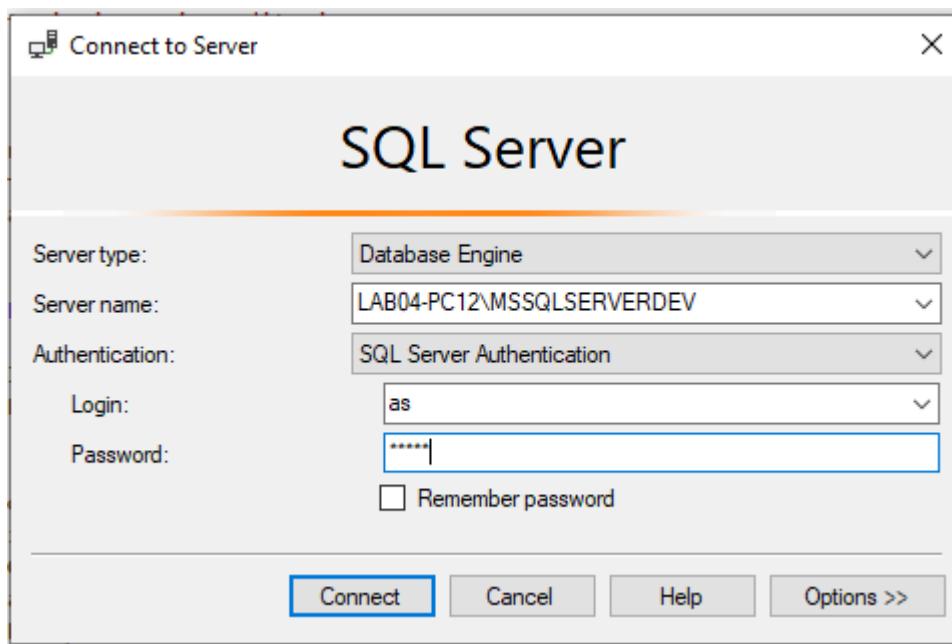
Prácticas seguras

- Preferir autenticación Windows cuando sea posible.
- Deshabilitar la cuenta sa o cambiarle el nombre.
- Usar conexiones cifradas (SSL/TLS) y limitar accesos por IP.

Resultado



La autenticación de windows no te pide credenciales



La autenticación de SQL si te pide credenciales para conectarte a la base de datos

2. Cuentas de servicio y configuración del servidor

Cuentas de servicio:

Son las cuentas bajo las cuales se ejecutan los servicios de SQL Server (Motor, Agente, etc.). Deben tener los permisos mínimos necesarios (principio de menor privilegio).

Configuración clave del servidor:

- Revisar opciones como xp_cmdshell, Ad Hoc Distributed Queries, y remote access.
- Usar sp_configure para ajustar parámetros de seguridad.

Ejemplo

```
EXEC sp_configure 'show advanced options', 1;
RECONFIGURE;
EXEC sp_configure 'xp_cmdshell', 0;
RECONFIGURE;
```

Resultado

	name	minimum	maximum	config_value	run_value
1	show advanced options	0	1	1	1

Propiedades de la base de datos - QhatuPeru

Seleccionar una página Script Ayuda

Nombre	Valor para principal	Valor para secundario
ACCELERATED_PLAN_FORCING	ON	PRIMARY
ASYNC_STATS_UPDATE_WAIT_AT...	OFF	PRIMARY
BATCH_MODE_ADAPTIVE_JOINS	ON	PRIMARY
BATCH_MODE_MEMORY_GRANT_F...	ON	PRIMARY
BATCH_MODE_ON_ROWSTORE	ON	PRIMARY
CE_FEEDBACK	ON	PRIMARY
DEFERRED_COMPILATION_TV	ON	PRIMARY
DOP_FEEDBACK	OFF	PRIMARY
DW_COMPATIBILITY_LEVEL	AUTO	PRIMARY
ELEVATE_ONLINE	OFF	N/A
ELEVATE_RESUMABLE	OFF	N/A
EXEC_QUERY_STATS_FOR_SCALA...	ON	PRIMARY
FORCE_SHOWPLAN_RUNTIME_PAR...	OFF	PRIMARY
GLOBAL_TEMPORARY_TABLE_AUT...	ON	N/A
IDENTITY_CACHE	ON	N/A
INTERLEAVED_EXECUTION_TVF	ON	PRIMARY
ISOLATE_SECURITY_POLICY_CARDI...	OFF	PRIMARY
LAST_QUERY_PLAN_STATS	OFF	PRIMARY
LEDGER_DIGEST_STORAGE_ENDP...	OFF	PRIMARY
LEGACY_CARDINALITY_ESTIMATION	OFF	PRIMARY
LIGHTWEIGHT_QUERY_PROFILING	ON	PRIMARY
MAXDOP	0	PRIMARY
MEMORY_GRANT_FEEDBACK_PER...	ON	PRIMARY

Aceptar Cancelar

3. Creación de roles fijos y personalizados

Roles fijos:

- SQL Server incluye roles predefinidos como db_datareader, db_datawriter, db_owner, etc.
- Se asignan según el nivel de acceso requerido.

Roles personalizados:

- Puedes crear roles específicos para tu aplicación o usuarios.
- Permiten una administración más granular.

Ejemplo

```
CREATE ROLE Auditor;
GRANT SELECT ON SCHEMA::dbo TO Auditor;
EXEC sp_addrolemember 'Auditor', 'usuario_auditor';
```

Resultado

The screenshot shows the 'Database Role Properties' dialog box for the role 'db_securityadmin'. The 'General' tab is selected. The 'Role name:' field contains 'db_securityadmin' and the 'Owner:' field contains 'dbo'. Under 'Schemas owned by this role:', 'db_accessadmin' is selected. In the 'Members of this role:' section, there are 'Add...' and 'Remove' buttons. The 'Connection' and 'Progress' panes are also visible.

Below the dialog box is a tree view of database users and roles:

- Usuarios
 - CajeroQhatu
 - ConsultaCliente
 - dbo
 - GerenteQhatu
 - guest
 - INFORMATION_SCHEMA
 - sys
 - usuario_proveedor
 - VendedorQhatu
- Roles
 - Roles de base de datos
 - db_accessadmin
 - db_backupoperator
 - db_datareader
 - db_datawriter
 - db_ddladmin
 - db_denydatareader
 - db_denydatawriter
 - db_owner
 - db_securityadmin
 - public
 - rol_proveedor_masked

4. Control de acceso mediante GRANT, DENY y REVOKE

GRANT: Otorga permisos.

DENY: Niega permisos explícitamente (tiene prioridad sobre GRANT).

REVOKE: Elimina permisos previamente otorgados.

Ejemplo:

```
GRANT SELECT ON dbo.Estudiantes TO Auditor;
DENY DELETE ON dbo.Estudiantes TO Auditor;
REVOKE SELECT ON dbo.Estudiantes FROM Auditor;
```

```
-- tabla con precios
USE QhatuPeru;

CREATE TABLE dbo.INVENTARIO (
    ID_PRODUCTO INT PRIMARY KEY IDENTITY(1,1),
    NOMBRE NVARCHAR(100),
    STOCK INT,
    PrecioProveedor DECIMAL(10,2),
    PrecioVenta DECIMAL(10,2)
);

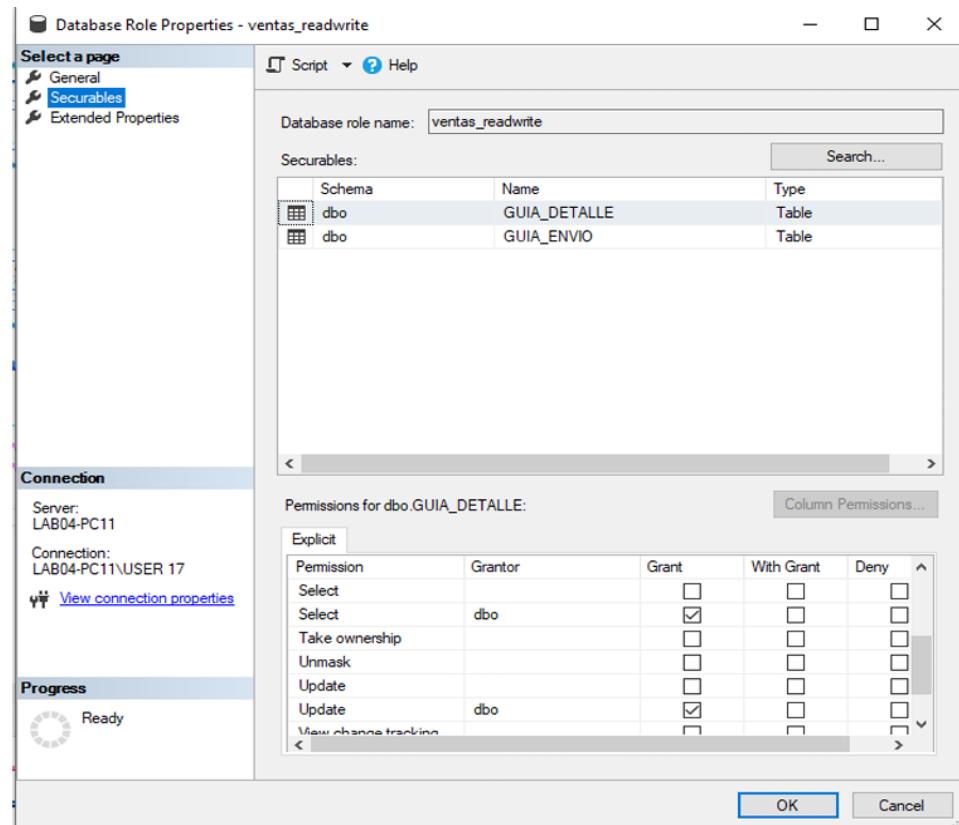
-- Crear login y usuario para el analista
CREATE LOGIN login_analista WITH PASSWORD = 'AnalistaSeguro2024!';
CREATE USER usuario_analista FOR LOGIN login_analista;

-- Crear rol de analista
CREATE ROLE rol_analista;
EXEC sp_addrolemember 'rol_analista', 'usuario_analista';

-- Conceder SELECT general sobre la tabla
GRANT SELECT ON dbo.INVENTARIO TO rol_analista;

-- Negar acceso a columnas sensibles
DENY SELECT ON dbo.INVENTARIO (PrecioProveedor, PrecioVenta) TO rol_analista;
```

RESULTADO



5. Cifrado y protección de datos (TDE, Always Encrypted)

TDE (Transparent Data Encryption):

- Cifra archivos de base de datos (.mdf, .ldf) en disco.
- Protege contra robo físico del archivo.

Always Encrypted:

- Cifra datos sensibles (como DNI, tarjetas) en columnas específicas.
- Los datos se cifran/desencRIPTAN en el cliente, no en el servidor.

Ejemplo:

```
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE MiCertificado;
ALTER DATABASE MiBD SET ENCRYPTION ON;

-- Paso 1: Crear master key en la base master
USE master;
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'ClaveSeguraMaster2024!';

-- Paso 2: Crear certificado de servidor
CREATE CERTIFICATE Certificado_QhatuPeru
WITH SUBJECT = 'Certificado para TDE en QhatuPeru';

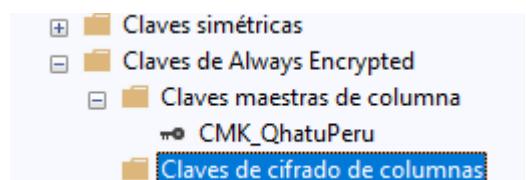
-- Paso 3: Crear la Database Encryption Key en la base QhatuPeru
USE QhatuPeru;
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_256
ENCRYPTION BY SERVER CERTIFICATE Certificado_QhatuPeru;

-- Paso 4: Activar el cifrado
ALTER DATABASE QhatuPeru
SET ENCRYPTION ON;

-- Verificar bases cifradas
SELECT name, is_encrypted
FROM sys.databases
WHERE name = 'QhatuPeru';

-- Verificar certificados
SELECT name, subject, expiry_date
FROM sys.certificates
WHERE name = 'Certificado_QhatuPeru';
```

RESULTADO



The screenshot shows the Results pane of SSMS. At the top, it says '100 %' and 'No se encontraron problemas.' (No problems found). Below this, there are two tabs: 'Resultados' and 'Mensajes'. The 'Resultados' tab contains a table with one row of data:

	name	is_encrypted
1	QhatuPeru	1

Below the results, there is another table with three columns: 'name', 'subject', and 'expiry_date'. This table is currently empty.

6. Auditoría y monitoreo de eventos con SQL Server Audit

SQL Server Audit:

- Permite registrar eventos como acceso a objetos, cambios de configuración, etc.
- Se configura a nivel de servidor o base de datos.

Pasos básicos:

1. Crear un objeto de auditoría.
2. Definir especificaciones (qué auditar).
3. Activar y revisar los logs.

Ejemplo

```
-- verificaciones
-- Auditorías a nivel servidor
SELECT name, audit_guid, is_state_enabled
FROM sys.server_audit_specifications;

-- Auditorías a nivel base de datos
SELECT name, is_state_enabled
FROM sys.database_audit_specifications;

CREATE SERVER AUDIT MiAuditoria
TO FILE (FILEPATH = 'C:\Auditorias\' );
CREATE SERVER AUDIT SPECIFICATION MiEspecificacion
FOR SERVER AUDIT MiAuditoria
ADD (SCHEMA_OBJECT_ACCESS_GROUP);
ALTER SERVER AUDIT MiAuditoria WITH (STATE = ON);
```

The screenshot shows the SQL Server Management Studio interface with two result sets displayed in tabs labeled 'Resultados' and 'Mensajes'. The 'Resultados' tab contains two tables. The first table, titled 'Resultados', has columns 'name', 'audit_guid', and 'is_state_enabled'. It shows one row for 'Audit_Logins' with audit_guid F498D3D4-3EDD-49D4-AE26-14610F90A16A and is_state_enabled 1. The second table, titled 'Mensajes', has columns 'name' and 'is_state_enabled'. It shows one row for 'Audit_DDL_QhatuPeru' with both columns set to 1.

	name	audit_guid	is_state_enabled
1	Audit_Logins	F498D3D4-3EDD-49D4-AE26-14610F90A16A	1

	name	is_state_enabled
1	Audit_DDL_QhatuPeru	1

Prácticas:

- Configurar auditoría para seguimiento de inicios de sesión.
- Implementar un esquema de cifrado para una columna sensible (ej. DNI o tarjeta).

1. Configurar auditoría para seguimiento de inicios de sesión

Registrar quién accede al servidor, cuándo y desde dónde, para detectar accesos no autorizados o patrones sospechosos.

```
//crear el objeto de auditoria
CREATE SERVER AUDIT AuditoriaLogins
TO FILE (FILEPATH = 'C:\Auditorias\Logins');

//Creamos la especificación de la auditoria
CREATE SERVER AUDIT SPECIFICATION EspecificacionLogins
FOR SERVER AUDIT AuditoriaLogins
ADD (SUCCESSFUL_LOGIN_GROUP),
ADD (FAILED_LOGIN_GROUP);

//Activamos la auditoria
ALTER SERVER AUDIT AuditoriaLogins WITH (STATE = ON);
```

```
USE master;
--paso 1 creamos el server audit
-- Crear el audit en el servidor, con archivo de salida
CREATE SERVER AUDIT Audit_QhatuPeru
TO FILE (FILEPATH = 'E:\SQLAudit\'')
WITH (ON_FAILURE = CONTINUE);

-- Habilitar el audit
ALTER SERVER AUDIT Audit_QhatuPeru
WITH (STATE = ON);

--paso 2
-- Registrar intentos de login
CREATE SERVER AUDIT SPECIFICATION Audit_Logins
FOR SERVER AUDIT Audit_QhatuPeru
ADD (SUCCESSFUL_LOGIN_GROUP),
ADD (FAILED_LOGIN_GROUP)
WITH (STATE = ON);

--paso 3
-- crear la database para cambios DDL
USE QhatuPeru;

CREATE DATABASE AUDIT SPECIFICATION Audit_DDL_QhatuPeru
FOR SERVER AUDIT Audit_QhatuPeru
ADD (SCHEMA_OBJECT_CHANGE_GROUP)
WITH (STATE = ON);
```

Con el código escrito ya estaría configurado y se generarían los archivos .sqlaudit

RESULTADO

Audit_QhatuPeru_F498D3D4-3EDD-49D4-... 13/11/2025 17:15 Archivo SQLAUDIT 496 KB

The screenshot shows a SQL Server Management Studio window with two result sets. The first result set is titled 'Resultados' and contains a table with three columns: name, audit_guid, and is_state_enabled. It has one row for 'Audit_Logins'. The second result set is titled 'Mensajes' and contains a table with two columns: name and is_state_enabled. It has one row for 'Audit_DDL_QhatuPeru'.

	name	audit_guid	is_state_enabled
1	Audit_Logins	F498D3D4-3EDD-49D4-AE26-14610F90A16A	1

	name	is_state_enabled
1	Audit_DDL_QhatuPeru	1

2. Implementar un esquema de cifrado para una columna sensible (ej. DNI o tarjeta)

Proteger datos sensibles como el número de DNI o tarjeta de crédito, incluso si alguien accede directamente a la base de datos. Usamos **Always Encrypted**, que cifra los datos en el cliente antes de enviarlos al servidor.

```
//Creamos una clave maestra en el almacen de certificados
//Creamos una clave de columna
CREATE COLUMN MASTER KEY MiClaveMaestra
WITH (
    KEY_STORE_PROVIDER_NAME = 'MSSQL_CERTIFICATE_STORE',
    KEY_PATH = 'CurrentUser/My/MiCertificado'
);

CREATE COLUMN ENCRYPTION KEY ClaveDNI
WITH VALUES (
    COLUMN_MASTER_KEY = MiClaveMaestra,
    ALGORITHM = 'RSA_OAEP',
    ENCRYPTED_VALUE = <valor_encriptado>
);

//Creamos la tabla columna cifrada
CREATE TABLE Ciudadanos (
    Id INT PRIMARY KEY,
    Nombre NVARCHAR(100),
    DNI CHAR(8) COLLATE Latin1_General_BIN2 ENCRYPTED WITH (
        COLUMN_ENCRYPTION_KEY = ClaveDNI,
        ENCRYPTION_TYPE = DETERMINISTIC,
        ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256'
    )
);

CREATE TABLE dbo.PROVEEDORES (
    ID_PROVEEDOR INT PRIMARY KEY IDENTITY(1,1),
    NOMBRE NVARCHAR(100),
    PrecioProveedor_ENC DECIMAL(10,2)
    COLLATE Latin1_General_BIN2
    ENCRYPTED WITH (
        COLUMN_ENCRYPTION_KEY = CEK_QhatuPeru,
        ENCRYPTION_TYPE = Randomized,
        ALGORITHM = 'AEAD_AES_256_CBC_HMAC_SHA_256'
    )
);
```

El cifrado **determinístico** permite búsquedas exactas (`WHERE DNI = '12345678'`).

El cifrado **aleatorio** es más seguro, pero no permite búsquedas directas.

RESULTADO

Nombre:

Clave maestra de columna:

Las claves de cifrado de columna protegen los datos y las claves maestras de columna protegen las claves de cifrado de columna. Esto le permite administrar menos claves.

Para crear una nueva clave maestra de columna, use la página 'Nueva clave maestra de columna'.

Nombre:

Clave maestra de columna: