

**1. Proteger Base de datos con Transparent Data Encryption.**

**a. Creé 2 bases de datos.**

```
--Creacion de bases de datos para prueba
CREATE DATABASE TEST_WITHOUT_ENCRYPTION
CREATE DATABASE TEST_ENCRYPTION
```

**b. Inserte los mismos datos en cada una.**

```
--Insercion de datos de prueba en la base de datos que sera encriptada.
USE TEST_ENCRYPTION
CREATE TABLE NAMES (
    ID INT IDENTITY(1,1) PRIMARY KEY,
    NAME VARCHAR(50) NOT NULL
)
INSERT INTO NAMES(
    NAME
)VALUES
    ('Martin'),
    ('Francisco')

--Insercion de datos de prueba en la base de datos que NO sera encriptada.
USE TEST_WITHOUT_ENCRYPTION
CREATE TABLE NAMES (
    ID INT IDENTITY(1,1) PRIMARY KEY,
    NAME VARCHAR(50) NOT NULL
)
INSERT INTO NAMES(
    NAME
)VALUES
    ('Martin'),
    ('Francisco')
```

**c. Pasos para encriptar.**

```
--Creacion del certificado y la clave
USE master;
GO
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'ThisIsAStrongPassword';
GO
CREATE CERTIFICATE MyServerCert WITH SUBJECT = 'My DEK Certificate';
GO

--Crea clave de encriptacion para el certificado
USE [TEST_ENCRYPTION]
GO
CREATE DATABASE ENCRYPTION KEY
WITH ALGORITHM = AES_128
ENCRYPTION BY SERVER CERTIFICATE MyServerCert;
GO

--Backup del certificado y la key
USE master
GO
BACKUP CERTIFICATE MyServerCert
TO FILE = 'D:\ArchivosImportantes\BackupsSQL\MyServerCert.cer'
WITH PRIVATE KEY (FILE = 'D:\ArchivosImportantes\BackupsSQL\MyCertKey.pvk', ENCRYPTION BY PASSWORD = 'ThisIsAStrongPassword')
GO

--Habilita la encriptacion de la base de datos
ALTER DATABASE [TEST_ENCRYPTION]
SET ENCRYPTION ON;
GO
```

#### d. Prueba de los certificados y la clave creada.

```
--Muestra los detalles de los certificados
USE master
GO
SELECT * FROM sys.certificates WHERE pvt_key_encryption_type <> 'NA'
GO

--Muestra los detalles de las claves
USE master
GO
SELECT encryptor_type, key_length, key_algorithm, encryption_state, create_date
FROM sys.dm_database_encryption_keys
GO
```

Results Messages

name	certificate_id	principal_id	pvt_key_encryption_type	pvt_key_encryption_type_desc	is_active_for_begin_dialog	issuer_name	cert_serial_nur
MyServerCert	258	1	MK	ENCRYPTED_BY_MASTER_KEY	1	My DEK Certificate	3d 63f2 37 7C

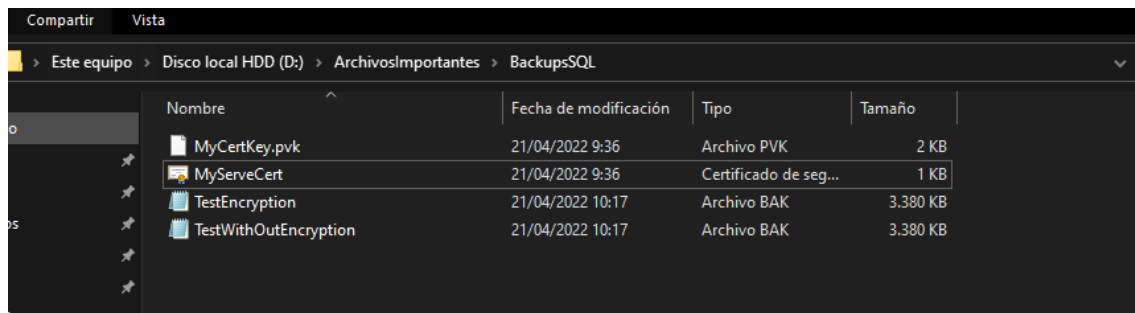
  

encryptor_type	key_length	key_algorithm	encryption_state	create_date
ASYMMETRIC KEY	256	AES	3	2022-04-21 15:12:07.430
CERTIFICATE	128	AES	3	2022-04-21 15:31:08.463

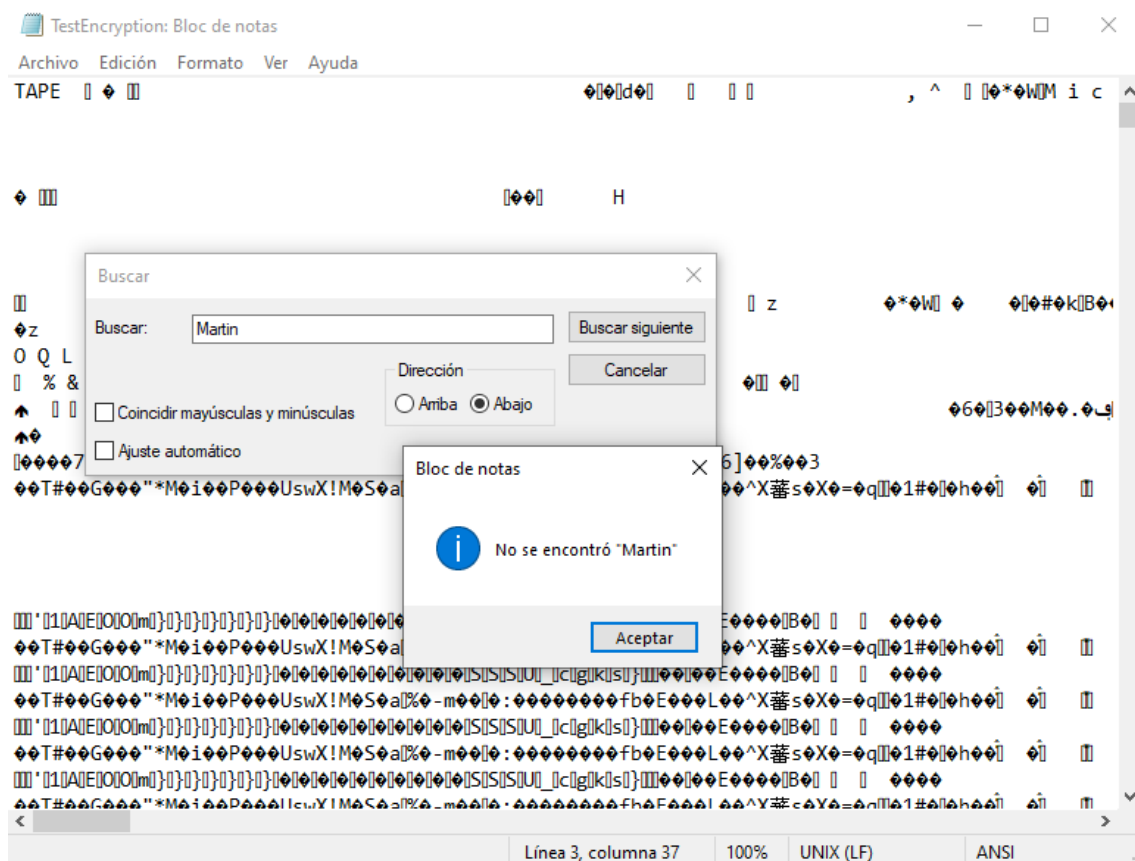
#### e. Creación de backups para mostrar la encriptación.

```
--Creacion de copias de seguridad
USE master
GO
BACKUP DATABASE [TEST_ENCRYPTION] TO DISK = 'D:\ArchivosImportantes\BackupsSQL\TestEncryption.bak'
GO

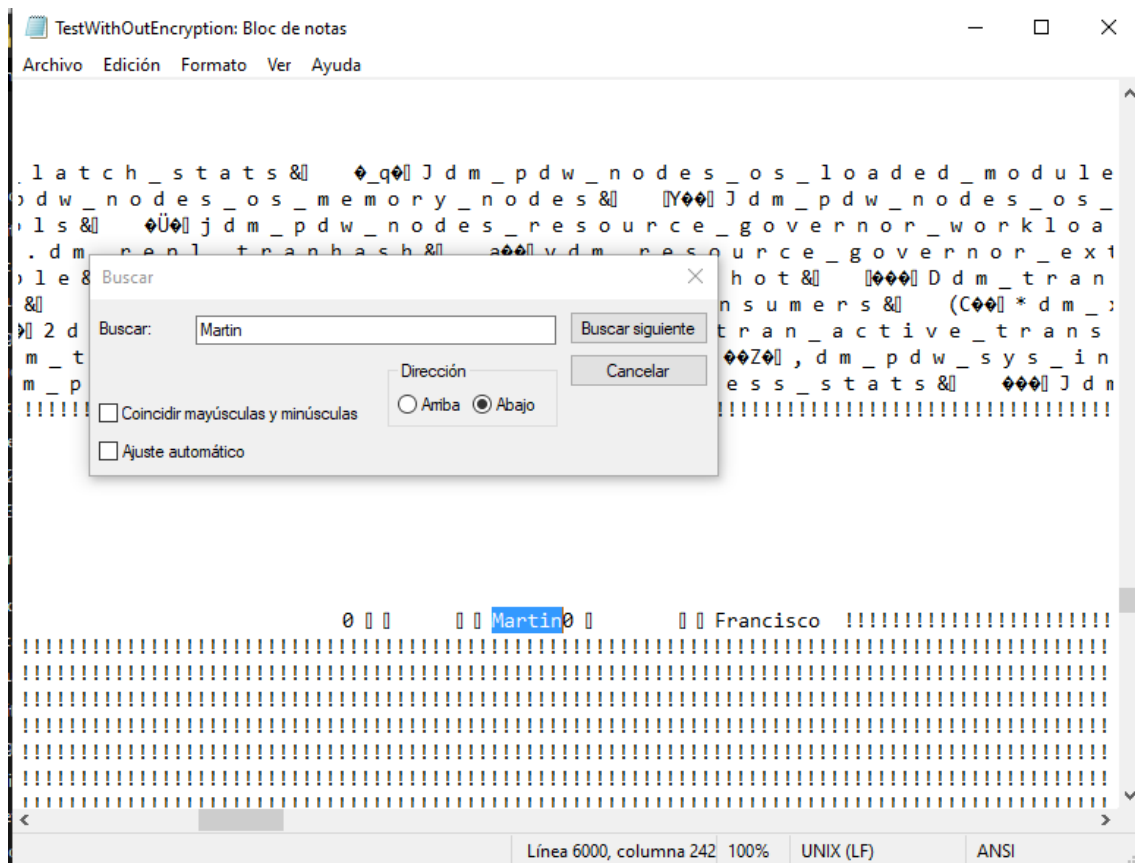
USE master
GO
BACKUP DATABASE [TEST_WITHOUT_ENCRYPTION] TO DISK = 'D:\ArchivosImportantes\BackupsSQL\TestWithOutEncryption.bak'
GO
```



## f. Inspección de backup con encriptación.



## g. Inspección de backup sin encriptación.



## 2. Descripción del mecanismo.

Este método de seguridad consta de una clave y un certificado para encriptar una base de datos. Al encriptar la base de datos queda protegida en caso de un ataque a esta ya que los datos en su interior no pueden ser consultados sin la respectiva clave y certificado.

Tanto el certificado como la clave deben ser guardados ya que estos son necesarios para acceder a los datos y lograr una correcta restauración de la base de datos.

Los archivos se cifran al ser escritos en el disco y se descifran al leerse en memoria, esto hace que el tamaño de los datos no aumente.

### **3. 2 ventajas.**

- a. Seguridad en caso de que sustraigan los medios de almacenamiento de la base de datos.
- b. Las operaciones de administración de claves están automatizadas, ya que se cifra al escribir en disco y se descifra al leer en memoria.

### **4. 2 desventajas.**

- a. Si también se sustrae la clave primaria y el certificado se podrá acceder a los datos fácilmente.
- b. Si se pierde ya sea la llave primaria o el certificado no se podrá restaurar la base de datos.

### **Bibliografía:**

ArcMap. (s. f.) *Cifrado transparente de datos (TDE) para el espacio de trabajo de revisor en SQL Server—Ayuda / Documentación.*

<https://desktop.arcgis.com/es/arcmap/10.3/guide-books/extensions/data-reviewer/transparent-data-encryption-tde-for-the-reviewer-workspace-in-sql-server.htm>

Microsoft. (2012). *Transparent Data Encryption (TDE)*. Microsoft Docs.

[https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2012/bb934049\(v=sql.1110\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2012/bb934049(v=sql.1110)?redirectedfrom=MSDN)