

UNIVERSIDAD PERUANA LOS ANDES
FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
Y COMPUTACIÓN



ENCRIPTAR DATOS EN SQL SERVER

Presentado por:

Gonzalo Aguilera Luis Angel

Docente:

Raúl Bejarano

Curso:

Base de Datos II

Sección:

A1

HUANCAYO – PERÚ

2024

Encriptado de Datos en SQL Server

El encriptado (o cifrado) es un proceso que convierte información legible en un formato ilegible para protegerla de accesos no autorizados. Este proceso es fundamental en la seguridad de la información y tiene varias aplicaciones importantes:

Propósitos del encriptado

1. Confidencialidad:

- El encriptado garantiza que solo las personas autorizadas puedan acceder y entender la información. Por ejemplo, los datos sensibles como contraseñas, información financiera y datos personales se cifran para protegerlos de terceros.

2. Integridad:

- Al cifrar datos, se puede verificar que la información no ha sido alterada durante la transmisión o el almacenamiento. Esto se logra mediante técnicas como el uso de hash, que pueden alertar si los datos han sido modificados.

Primero creamos una tabla **USUARIOS**

```
-- ***** --  
-- **          ENCRYPTAR Y DESENCRIPTAR CONTRASEÑAS          ** --  
-- ***** --  
  
CREATE TABLE USUARIOS
```

1. Creamos un campo usuario lo cual tendrá su respectivo campo de PASSWORD sin encriptar y también con su encriptación.

```
(USUARIO VARCHAR(30) PRIMARY KEY,  
PASSWORD_SIN_ENCRYPTAR VARCHAR(15),  
PASSWORD_ENCRYPTADO VARBINARY(255)) -- TIPO DE CAMPO PARA ENCRYPTAR
```

2. Ahora encriptamos por frase:

```
-- ENCRYPTAR POR FRASE  
  
INSERT INTO USUARIOS VALUES  
('jbedoyar', 'Santy2002', ENCRYPTBYPASSPHRASE('password', 'Santy2002'))
```

Introducimos un valor, el nombre y la contraseña sin encriptar **Santy2002** y para poder encriptar utilizamos el procedimiento de **ENCRYPTBYPASSPHRASE** acompañado de una **frase + la contraseña o dato a encriptar**

3. Ahora seleccionamos la tabla para poder visualizar los datos.

```
INSERT INTO USUARIOS VALUES  
('jbedoyar', 'Santy2002', ENCRYPTBYPASSPHRASE('password', 'Santy2002'))  
  
SELECT * FROM USUARIOS
```

4. Ahora logramos visualizar los datos que agregamos hace un momento:

Results		Messages
USUARIO	PASSWORD_SIN_ENCRYPTAR	PASSWORD_ENCRYPTADO
1	jbedoyar	Santy2002
		0x02000000174B9031B1DAB97838D219E6C0CAB21BD55690...

AHORA DESENCRIPTAREMOS POR FRASE

1. Primero Agregamos mas Usuarios a la tabla que tenemos:

```
INSERT INTO USUARIOS VALUES  
('pandrea', 'sarita2015', ENCRYPTBYPASSPHRASE('password', 'sarita2015'))  
  
INSERT INTO USUARIOS VALUES  
('sarabed', 'sarabed', ENCRYPTBYPASSPHRASE('password', 'sarabed'))
```

y ahora encriptaremos un ultimo valor pero con una **frase diferente**:

```
INSERT INTO USUARIOS VALUES  
('santybed', 'sbedoyar', ENCRYPTBYPASSPHRASE('password1', 'sbedoyar'))
```

Teniendo la siguiente tabla:

Results		Messages
USUARIO	PASSWORD_SIN_ENCRYPTAR	PASSWORD_ENCRYPTADO
1	jbedoyar	Santy2002
		0x02000000174B9031B1DAB97838D219E6C0CAB21BD55690...
2	pandrea	sarita2015
		0x02000000DA226163E6F29293A5D43DB43DAF96183CDA8...
3	santybed	sbedoyar
		0x0200000074214FEA1A1752A1E63A211B9D0407202F6FAE7...
4	sarabed	sarabed
		0x020000007DB858E6173EFED4DFFCEBA8B0A518527E454...

2. Ahora desencryptaremos a todos los datos con el siguiente comando:

```
SELECT USUARIO, PASSWORD_SIN_ENCRYPTAR,  
CONVERT(VARCHAR(50), DECRYPTBYPASSPHRASE('password', PASSWORD_ENCRIP  
FROM USUARIOS
```

3. Teniendo los siguientes datos:

Results		Messages
USUARIO	PASSWORD_SIN_ENCRYPTAR	(No column name)
1	jbedoyar	Santy2002
2	pandrea	sarita2015
3	santybed	sbedoyar
4	sarabed	sarabed

- Podemos observar que se descripto todos los datos menos 1, esoe dato lo encriptamos con una frase diferente al resto, por ello no se puede visualizar la contraseña.