

Capítulo 6: Administración múltiples servidores

Capítulo 7: Protección de los datos

Capítulo 8: Alta disponibilidad con AlwaysOn



7

Protección de datos

SQL Server 2016 - Nivel Avanzado

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.




Objetivos

- Identificar las diferentes áreas expuestas que deben ser aseguradas.
- Asegurar datos a nivel granular.
- Asegurar bases de datos a nivel global.
- Minimizar el riesgo de accesos no autorizados.
- Minimizar el riesgo de fugas de información.

7 - 2

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Agenda

- Integración con políticas de seguridad de Windows Server
- Seguridad de los servicios
- Encriptado de datos
- Implementando encriptación a nivel de celda
- Encriptado transparente de datos (TDE)
- Enmascarado dinámico de datos

7 - 3

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Integración con políticas de seguridad de Windows Server

Integración de políticas de seguridad de Windows Server con SQL Server.

La directiva de grupo define los requisitos de contraseña de Windows:

- Longitud
- Complejidad
- Expiración
- Repetición

SQL Server aplica la directiva de contraseña solo a los inicios de sesión de SQL.

Requiere SQL Server 2005 o superior, y Windows Server 2008 o superior.

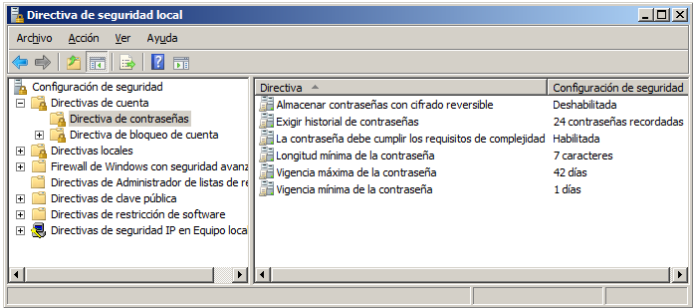
7 - 4

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Integración con políticas de seguridad de Windows Server

Las políticas de clave de seguridad se definen a través de las directivas de seguridad local de Windows Server, opción directivas de cuenta, directivas de contraseña:



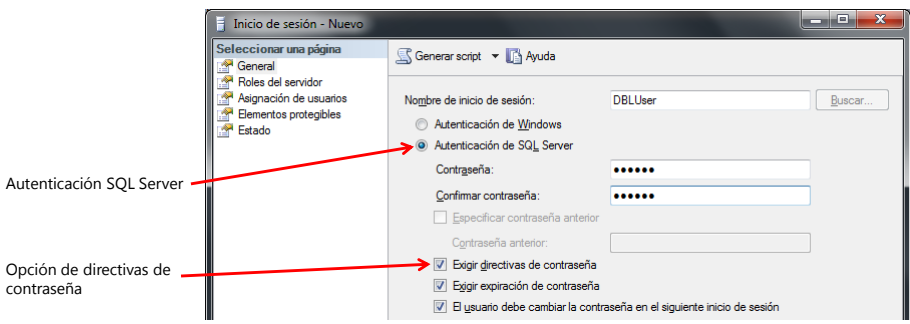
7 - 5

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Integración con políticas de seguridad de Windows Server

En el proceso de creación de un inicio de sesión de SQL Server, se especifica si se va a integrar la política de clave.



7 - 6

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Seguridad de los servicios

- Un servicio de SQL Server es un proceso independiente que interactúa con el sistema operativo para ejecutar tareas del motor de base de datos, de servicios de análisis integración, reportes, etc.
- La interacción implica autenticación de una cuenta, llamada cuenta del servicio.
- Aislar los servicios reduce el riesgo de que un servicio comprometido pueda afectar a los demás servicios.
- Para aislar servicios considere ejecutar cada servicio SQL Server usando cuentas separadas de Windows.
- Usar cuentas de dominio de Windows o locales con bajos privilegios.

7 - 7

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Seguridad de los servicios

Los siguientes servicios pueden ser instalados con SQL Server:

- SQL Server Database
- SQL Server Agent
- Analysis Services
- Reporting Services
- Integration Services
- SQL Server Browser
- Full-text search
- SQL Writer
- SQL Server Distributed Replay Controller
- SQL Server Distributed Replay Client



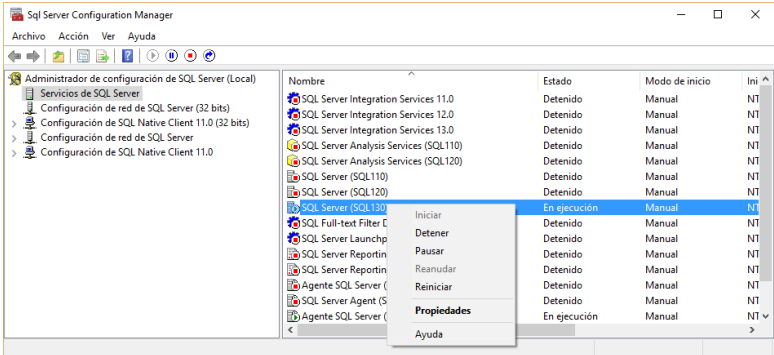
7 - 8

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Seguridad de los servicios

- Para administrar los servicios se utiliza SQL Server Configuration Manager.
- La cuenta del servicio se configura a través de las propiedades del servicio.



7 - 9

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.

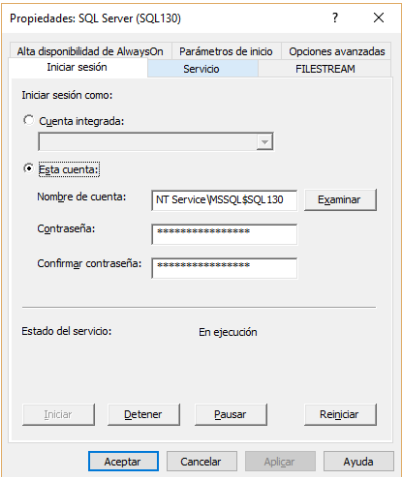


Seguridad de los servicios

En las propiedades del servicio, se cuenta con la página iniciar sesión.

Se configura el tipo de cuenta:

- Cuenta integrada
 - Sistema local
 - Servicio local
 - Servicio de red
- Cuenta de Windows
 - Dominio (**mejor práctica**)
 - Local



7 - 10

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Ejercicio Nº 7.1: Configurar la seguridad de los servicios de SQL Server

Asegurar los servicios de SQL Server, así como los datos almacenados en las bases de datos.

Al finalizar el capítulo, el alumno logrará:

- Configurar el servicio:
 - Verificar cuenta de dominio.
 - Asignar cuenta de dominio al servicio de SQL Server.
 - Asignar cuenta de dominio al servicio de SQL Server Agent.

7 - 11

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

- El encriptado de datos eleva la seguridad de la información de SQL Server
- Motivos para encriptar datos:
 - Privacidad.
 - Cumplimiento de regulaciones.
- El encriptado se produce a través de algoritmos.
- El algoritmo define la transformación de los datos.
- Dicha transformación no puede ser fácilmente reversada por usuarios no autorizados.

7 - 12

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

SQL Server ofrece una variedad de algoritmos de encriptado:

- DES
- Triple_DES
- TRIPLE_DES_3KEY
- DESX
- 128-bit AES
- 192-bit AES
- 256-bit AES
- RC2 (mantenido solo por compatibilidad con SQL 2005)
- RC4 (mantenido solo por compatibilidad con SQL 2005)
- 128-bit RC4 (mantenido solo por compatibilidad con SQL 2005)

7 - 13

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

- En encriptado implica:
 - Proceso de cifrado al momento de escribir.
 - Proceso de descifrado al momento de leer.
- Esto recarga el procesador, provocando una disminución en los tiempos de respuesta.
- Dependiendo del algoritmo seleccionado, mientras más fuerte sea el algoritmo, mas CPU se consume, pero mayor seguridad de los datos.
- Don niveles de encriptado en SQL Server:
 - A nivel de celda.
 - A nivel de base de datos.

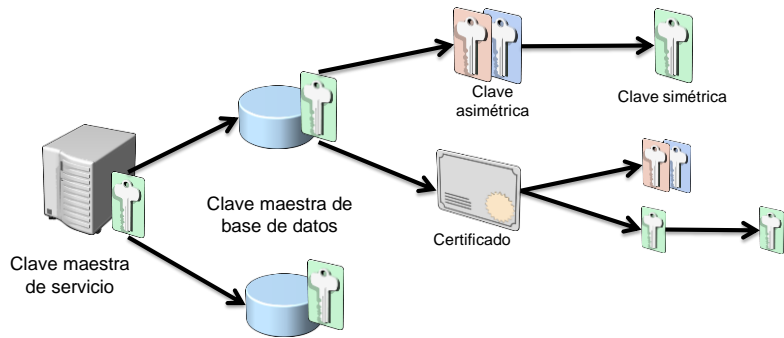
7 - 14

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

Arquitectura de criptografía de SQL Server



7 - 15

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

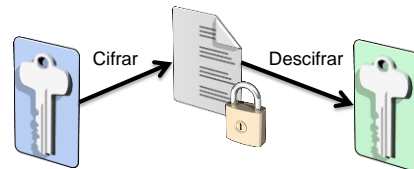
Claves

Simétrica

- La misma clave se usa para cifrar y descifrar.

Asimétrica

- Pareja de valores: clave pública y clave privada.
- Una cifra y la otra descifra.



7 - 16

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.

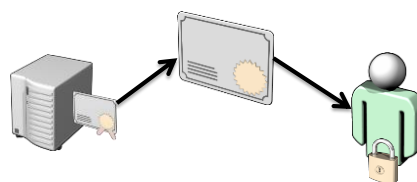


Encriptado de datos

Certificados

Contenido:

- Información identificadora del sujeto.
- Período de validez.
- Información identificadora y firma digital del emisor.



7 - 17

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado de datos

Usar llaves para:

- Asegurar los datos, ya sea a nivel de celda o de base de datos.
- Encriptar texto plano.
- Asegurar llaves simétricas.

Usar certificados para:

- Asegurar conexiones en bases de datos reflejadas.
- Para firmar paquetes.
- Encriptar datos o conexiones.

7 - 18

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

Pasos para implementar encriptado a nivel de celda

- 1 Crear una llave maestra
- 2 Crear u obtener un certificado, protegido por la llave maestra
- 3 Crear una llave de encriptado de base de datos protegida por el certificado, para un usuario
- 4 Implementar rutinas de encriptado y desencriptado

7 - 19

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

1 Crear una llave maestra

- Llave simétrica creada para crear los demás objetos de seguridad del servidor.
- Encriptada mediante algoritmo AES_256.
- Se asigna una clave, mientras más larga y compleja la clave, mejor será la seguridad.

CREATE MASTER KEY ENCRYPTION

BY PASSWORD = 'Mientr@sM@sLargaYC0mplej@La#Clave-Mejor'

7 - 20

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

2 Crear u obtener un certificado, protegido por la llave maestra

- Objeto de seguridad a nivel de base de datos.
- Estándar de seguridad X.509.

```
CREATE CERTIFICATE CypherCert01  
WITH SUBJECT = 'Certificado para cifrado de datos'
```

7 - 21

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

3 Crear una llave de encriptado de base de datos protegida por el certificado

- Requerida para poder implementar TDE en la base de datos.
- Utiliza un certificado para proteger los datos.
- Especificar algoritmo de encriptado.

```
CREATE DATABASE ENCRYPTION KEY  
WITH ALGORITHM = TRIPLE_DES  
ENCRYPTION BY SERVER CERTIFICATE CypherCert01
```

7 - 22

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

4 Implementar rutinas de encriptado y desencriptado

- Basadas en funciones de encriptado y desencriptado.
- En el mismo proceso por lote (batch) se debe abrir la llave antes y cerrarla después de encriptar o desencriptar:
`OPEN SYMMETRIC KEY DBSimKey`
 --Usar las funciones de encriptado y desencriptado
`CLOSE ALL SYMMETRIC KEYS`
- Funciones retornan datos de tipo varbinary, por lo que se recomienda que la columna encriptada tenga ese tipo de dato.
- Si la columna tiene otro tipo de dato se debe usar conversión explícita con CAST o CONVERT.

7 - 23

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Implementando encriptación a nivel de celda

4 Implementar rutinas de encriptado y desencriptado

Funciones de encriptado y desencriptado:

- ENCRYPTEDBYKEY
 - Encripta los datos usando la llave simétrica de la base de datos.
`EncryptByKey (key_GUID , { 'cleartext' | @cleartext })`
- DECRYPTEDBYKEY
 - Desencripta los datos usando la llave simétrica de la base de datos.
`DecryptByKey ({ 'ciphertext' | @ciphertext })`

7 - 24

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado transparente de datos

- Cifrado completo de la base de datos.
- Ejecuta cifrado de entrada y salida (I/O) en tiempo real, tanto en los archivos de datos con los de registro de transacciones.
- Su implementación es transparente a los usuarios y a las aplicaciones.
- Si se mueven los archivos a otra instancia, estos no se pueden adjuntar.
- No se puede restaurar una copia de seguridad en otra instancia.
- Si se desea mover o restaurar en otra instancia, se deben implementar los mismos objetos de seguridad (Certificados y llaves) de la instancia original.

7 - 25

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado transparente de datos

Pasos para implementar TDE

- 1 Crear una llave maestra
- 2 Crear u obtener un certificado, protegido por la llave maestra
- 3 Crear una llave de encriptado de base de datos protegida por el certificado
- 4 Configurar la base de datos para usar encriptado

7 - 26

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Encriptado transparente de datos

4 Configurar la base de datos para usar encriptado

- Mediante el comando ALTER DATABASE se habilita TDE.
- La base de datos debe contener el certificado y la llave.

```
ALTER DATABASE WideWorldImporters  
SET ENCRYPTION ON
```

7 - 27

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Ejercicio Nº 7.2: Configurar encriptado transparente de datos

Asegurar los servicios de SQL Server, así como los datos almacenados en las bases de datos.

Al finalizar el capítulo, el alumno logrará:

- Encriptar la base de datos.
 - Crear llave maestra.
 - Crear certificado.
 - Crear llave de base de datos.
 - Validar encriptado.

7 - 28

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Enmascarado dinámico de datos

La nueva funcionalidad de enmascarado se implementa al momento de crear una tabla. Para cada campo que queremos enmascarar se utiliza la sentencia MASKED WITH. Junto con dicha sentencia hay que utilizar una función. Tenemos 4 funciones a disposición:

- Default.- Enmascarado total de acuerdo con los tipos de datos de los campos designados. Muestra el valor mínimo posible según el tipo de dato.
- Email.- Muestra la primera letra del correo electrónico y el sufijo “.com”
- Aleatorio (random).-Para datos numéricos; muestra un valor aleatorio entre un rango mínimo y máximo.
- Personalizado (partial).-Para datos de tipo cadena; muestra la primera y última letra y en el medio un carácter personalizado.

Si la tabla ya existe se utilizan el comando ALTER TABLE ...ALTER COLUMN para incluir el enmascarado.

7 - 29

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Enmascarado dinámico de datos

Ejemplo de uso de funciones de enmascarado dinámico.

```
CREATE TABLE dbo.Empleado (  
EmpleadoID int IDENTITY PRIMARY KEY,  
Nombre varchar(100) NOT NULL,  
Direccion varchar(100) MASKED WITH (FUNCTION = 'PARTIAL(1,"???",0)') NOT NULL,  
FlagDeConfianza bit MASKED WITH (FUNCTION = 'DEFAULT()') NULL,  
Email varchar(100) MASKED WITH (FUNCTION = 'EMAIL()') NULL,  
FechaUltimoAscenso date MASKED WITH (FUNCTION = 'DEFAULT()') NULL,  
Salario decimal(15,2) MASKED WITH (FUNCTION = 'DEFAULT()') NULL,  
Bono decimal(15,2) MASKED WITH (FUNCTION = 'RANDOM(10,100)') NULL);
```

Visualización con máscara

	EmpleadoID	Nombre	Direccion	FlagDeConfianza	Email	FechaUltimoAscenso	Salario	Bono
1	1	Ana Ramirez	C???	0	aXXX@XXX.com	1900-01-01	0.00	23.15
2	2	Guillermo Ruiz	C???	0	gXXX@XXX.com	NULL	0.00	NULL

Visualización sin máscara

	EmpleadoID	Nombre	Direccion	FlagDeConfianza	Email	FechaUltimoAscenso	Salario	Bono
1	1	Ana Ramirez	Calle 1 123 Surquillo	0	aramirez@dblearner.com	2016-05-15	2800.00	300.00
2	2	Guillermo Ruiz	Calle 2 321 Lince	1	gruiz@dblearner.com	NULL	2400.00	NULL

7 - 30

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Enmascarado dinámico de datos

- Los usuarios de base de datos que forman parte del rol db_owner podrán visualizar los datos aun si están enmascarados
- Si se desea que un usuario que no pertenece al rol db_owner también visualice los datos enmascarados, se puede usar el permiso UNMASK

```
--OTORGAR PERMISO DE UNMASK (QUITAR MASCARA AL USUARIO)  
GRANT UNMASK TO Analista;
```

```
--REVOCAR PERMISO DE UNMASK (REPONER LA MASCARA AL USUARIO)  
REVOKE UNMASK TO Analista;
```

7 - 31

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Ejercicio N° 7.3: Implementar enmascarado dinámico de datos

Asegurar los servicios de SQL Server, así como los datos almacenados en las bases de datos.

Al finalizar el capítulo, el alumno logrará:

- Implementar una tabla con máscara de datos.
 - Crear la tabla.
 - Consultar los datos con máscara.
 - Consultas los datos sin máscara.

7 - 32

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Tarea Nº 7: Protección de datos

Aplicar teorías de protección de datos

- Identifique en su organización, si existe información sensible que debe ser protegida con cifrado de datos. Explique.
- Describa la jerarquía de cifrado de SQL Server.
- Identifique los algoritmos de cifrado soportados por SQL Server y haga una breve explicación de cada uno de ellos.
- Identifique los elementos de la arquitectura de cifrado transparente de SQL Server (no es necesario explicar cada uno).

7 - 33

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Lecturas adicionales

Para obtener información adicional, puede consultar:

- [Información general sobre seguridad de SQL Server](#)
- [Proteger SQL Server](#)
- [Directiva de contraseñas](#)
- [Cuenta de inicio del servicio para SQL Server](#)
- [Cifrado de SQL Server](#)
- [Jerarquía de cifrado de SQL Server](#)
- [Cifrar una columna de datos](#)
- [Cifrado de datos transparente \(TDE\)](#)

7 - 34

Copyright © Todos los Derechos Reservados - Cibertec Perú SAC.



Resumen

- Integración con políticas de seguridad de Windows Server
- Seguridad de los servicios
- Encriptado de datos
- Implementando encriptación a nivel de celda
- Encriptado transparente de datos (TDE)
- Enmascarado dinámico de datos

