

CEPSUNI

www.ceps.uni.edu.pe

UNIDAD 02 – Laboratorio 03

GESTION DE LA SEGURIDAD



Microsoft®
SQL Server®

GUSTAVO CORONEL

www.youtube.com/c/DesarrollaSoftware

gcoronel@uni.edu.pe

Temas

1	PROTEGER SQL SERVER	4
1.1	SEGURIDAD DE LA PLATAFORMA Y LA RED.....	4
1.1.1	<i>Seguridad física.....</i>	4
1.1.2	<i>Seguridad del sistema operativo</i>	4
1.1.3	<i>Seguridad de los archivos del sistema operativo de SQL Server.....</i>	5
1.2	ENTIDADES DE SEGURIDAD Y SEGURIDAD DE OBJETOS DE BASE DE DATOS	5
1.2.1	<i>Cifrado y certificados</i>	5
1.3	SEGURIDAD DE LAS APLICACIONES	5
1.4	HERRAMIENTAS, UTILIDADES, VISTAS Y FUNCIONES DE SEGURIDAD DE SQL SERVER.....	6
1.4.1	<i>Herramientas y utilidades de seguridad de SQL Server</i>	6
1.4.2	<i>Funciones y vistas de catálogo de seguridad de SQL Server</i>	6
2	ENTIDADES DE SEGURIDAD	7
2.1	INICIO DE SESIÓN SA DE SQL SERVER	7
2.2	ROL DE BASE DE DATOS PUBLIC.....	8
2.3	INFORMATION_SCHEMA Y SYS	9
2.4	USUARIO GUEST	10
3	PERMISOS	11
3.1	CONVENCIONES DE NOMENCLATURA DE PERMISOS	11
3.2	PERMISOS APLICABLES A ELEMENTOS PROTEGIBLES ESPECÍFICOS	13
3.3	DIRECTORES (PRINCIPALS)	14
3.4	ASEGURABLES (SECURABLES).....	14
3.5	PERMISOS	14
4	SEGURIDAD A NIVEL DEL SERVIDOR.....	15
4.1	TIPOS DE AUTENTICACIÓN	15
4.2	MODOS DE AUTENTICACIÓN	15
4.3	POLÍTICAS DE MANEJO DE CONTRASEÑAS	15
4.4	CREACIÓN DE UN INICIO DE SESIÓN.....	15
4.5	ROL FIJO DE SERVIDOR.....	16
4.6	SUPLANTACIÓN O DELEGACIÓN	16
4.7	CREDENCIALES	16
4.8	CONCESIÓN DE PERMISOS	16
5	SEGURIDAD A NIVEL DE LA BASE DE DATOS	17
5.1	USUARIOS	17
5.2	USUARIO DBO.....	17
5.3	USUARIO GUEST	17
5.4	ROL DE BASE DE DATOS	17

5.5	EL ROL DE BASE DE DATOS PUBLIC.....	18
5.6	ROL DE APLICACIÓN.....	18
6	CURSOS RELACIONADOS	19

1 PROTEGER SQL SERVER

1.1 Seguridad de la plataforma y la red

La plataforma de SQL Server incluye el hardware físico y los sistemas de redes que conectan los clientes con los servidores de bases de datos, así como los archivos binarios que se utilizan para procesar solicitudes de base de datos.

1.1.1 Seguridad física

Las recomendaciones de seguridad física limitan de forma estricta el acceso al servidor físico y a los componentes de hardware. Se debe usar salas cerradas de acceso restringido para el hardware de servidor de base de datos y los dispositivos de red. Además, se debe limitar el acceso a los medios de copia de seguridad almacenándolos en una ubicación segura fuera de las instalaciones.

La implementación de la seguridad de la red física comienza por mantener a los usuarios no autorizados fuera de la red.

1.1.2 Seguridad del sistema operativo

Los **Service Packs** y las actualizaciones del sistema operativo incluyen mejoras de seguridad importantes. Se debe aplicar todas las revisiones y actualizaciones al sistema operativo después de probarlas con las aplicaciones de base de datos.

Los **firewalls** también proporcionan formas eficaces de implementar la seguridad. Un firewall es un separador o limitador del tráfico de red, que puede configurarse para aplicar la directiva de seguridad de datos de una organización. Si se utiliza un firewall, aumentará la seguridad del sistema operativo, ya que proporciona un cuello de botella en el que pueden concentrarse las medidas de seguridad.

La reducción del área expuesta es una medida de seguridad que implica detener o deshabilitar los componentes que no se utilizan. La reducción del área expuesta ayuda a mejorar la seguridad al proporcionar menos accesos para potenciales ataques al sistema.

1.1.3 Seguridad de los archivos del sistema operativo de SQL Server

SQL Server usa archivos del sistema operativo para su funcionamiento y el almacenamiento de datos. Las recomendaciones de seguridad de archivos indican que se restrinja el acceso a estos archivos. Los Service Packs y actualizaciones de SQL Server proporcionan una seguridad mejorada.

El siguiente script permite averiguar el Service Pack instalado en el sistema:

```
SELECT CONVERT(char(20), SERVERPROPERTY('productlevel')) ;  
GO
```

1.2 Entidades de seguridad y seguridad de objetos de base de datos

Las **entidades de seguridad** son los individuos, grupos y procesos que tienen acceso a SQL Server. Los "**elementos protegibles**" son el servidor, la base de datos y los objetos incluidos en la base de datos. Cada uno de estos elementos dispone de un conjunto de permisos que pueden configurarse para reducir el área expuesta de SQL Server.

1.2.1 Cifrado y certificados

El cifrado no resuelve los problemas de control de acceso. Sin embargo, mejora la seguridad debido a que limita la pérdida de datos, incluso en el caso poco probable de que se superen los controles de acceso. Por ejemplo, si el equipo host de base de datos no está configurado correctamente y un usuario malintencionado obtiene datos confidenciales, como números de tarjetas de crédito, esa información robada podría resultar inservible si está cifrada.

Los certificados son "claves" de software que se comparten entre dos servidores que habilitan las comunicaciones seguras a través de una autenticación segura. Puede crear y usar certificados en SQL Server para mejorar la seguridad de objetos y conexiones.

1.3 Seguridad de las aplicaciones

Las recomendaciones de seguridad de SQL Server incluyen la creación de aplicaciones cliente seguras.

1.4 Herramientas, utilidades, vistas y funciones de seguridad de SQL Server

SQL Server proporciona herramientas, utilidades, vistas y funciones que pueden utilizarse para configurar y administrar la seguridad.

1.4.1 Herramientas y utilidades de seguridad de SQL Server

En la siguiente tabla se incluye información acerca de las herramientas y utilidades de SQL Server que se pueden utilizar para configurar y administrar la seguridad.

Herramienta / Utilidad	Descripción
SQL Server Management Studio	Permite conectarse, configurar y controlar SQL Server
sqlcmd (utilidad)	Consola de comandos en modo texto que permite conectarse y ejecutar consultas en un servidor SQL Server.
Administrador de configuración de SQL Server	Control y configuración de red para SQL Server.

1.4.2 Funciones y vistas de catálogo de seguridad de SQL Server

El Motor de base de datos expone información de seguridad en varias vistas y funciones que se optimizan en cuanto a rendimiento y utilidad. En la siguiente tabla se incluye información acerca de las funciones y vistas de seguridad.

Funciones / Vistas	Descripción
Vistas de catálogo de seguridad (Transact-SQL)	Vistas de catálogo de seguridad de SQL Server, que devuelven información sobre permisos de base de datos y servidor, entidades de seguridad, roles, etc. También hay vistas de catálogo que proporcionan información acerca de las claves de cifrado, los certificados y las credenciales.
Funciones de seguridad (Transact-SQL)	Funciones de seguridad de SQL Server, que devuelven información sobre el usuario, los permisos y los esquemas actuales.
Funciones y vistas de administración dinámica relacionadas con la seguridad (Transact-SQL)	Vistas de administración dinámica de seguridad de SQL Server.

2 ENTIDADES DE SEGURIDAD

Las entidades de seguridad son entidades que pueden solicitar recursos de SQL Server. Igual que otros componentes del modelo de autorización de SQL Server, las entidades de seguridad se pueden organizar en jerarquías. El ámbito de influencia de una entidad de seguridad depende del ámbito de su definición: Windows, servidor o base de datos; y de si la entidad de seguridad es indivisible o es una colección. Un Inicio de sesión de Windows es un ejemplo de entidad de seguridad indivisible y un Grupo de Windows es un ejemplo de una del tipo colección. Toda entidad de seguridad tiene un identificador de seguridad (SID).

- Entidades de seguridad a nivel de Windows
 - Inicio de sesión del dominio de Windows
 - Inicio de sesión local de Windows
- Entidades de seguridad de nivel de SQL Server
 - Inicio de sesión de SQL Server
 - Rol de servidor
- Entidades de seguridad de nivel de bases de datos
 - Usuario de la base de datos
 - Rol de base de datos
 - Rol de aplicación

2.1 Inicio de sesión SA de SQL Server

El inicio de sesión **sa** de SQL Server es una entidad de seguridad a nivel de servidor. Se crea de forma predeterminada cuando se instala una instancia. La base de datos predeterminada de **sa** es master.

Ejemplo 1

```
select
    name "LOGIN",
    default_database_name "DATABASE",
    default_language_name "LANGUAGE"
from sys.sql_logins
where name = 'sa';
go
```

2.2 Rol de base de datos PUBLIC

Todos los usuarios de una base de datos pertenecen al rol de base de datos **public**. Cuando a un usuario no se le han concedido ni denegado permisos para un elemento protegible, el usuario hereda los permisos para ese elemento concedidos a **public**.

Ejemplo 2

El siguiente script se debe ejecutar con el inicio de sesión **sa**

```
USE EduTec
GO

CREATE USER gustavo FOR LOGIN gustavo
GO
```

El siguiente script se debe ejecutar con el inicio de sesión **gustavo**:

```
USE EduTec
GO

select * from dbo.curso
GO
```

El siguiente script se debe ejecutar con el inicio de sesión **sa**

```
use EduTec
GO

GRANT SELECT ON dbo.Curso TO public
GO
```

A partir de este momento cualquier usuario que tenga acceso a la base de datos EduTec puede consultar la tabla CURSO.

El siguiente script se debe ejecutar con el inicio de sesión **gustavo**:

```
USE EduTec
GO

select * from dbo.curso
GO
```

2.3 INFORMATION_SCHEMA y SYS

Todas las bases de datos incluyen dos entidades que aparecen como usuarios en las vistas de catálogo: INFORMATION_SCHEMA y SYS. SQL Server necesita estas dos entidades. No son entidades de seguridad y no se pueden modificar ni quitar.

Ejemplo 3

En el siguiente ejemplo se consulta las tablas de una base de datos utilizando diferentes opciones.

Utilizando INFORMATION_SCHEMA:

```
use EduTec
GO

select * from INFORMATION_SCHEMA.TABLES
GO
```

Utilizando SYS:

```
use EduTec
GO

select * from SYS.TABLES
GO
```

Utilizando SYSOBJECT:

```
use EduTec
GO

SELECT * FROM sysobjects
WHERE xtype = 'U'
GO
```

2.4 Usuario GUEST

Cada base de datos incluye un usuario **GUEST**. Los permisos concedidos al usuario **guest** se aplican a todos los usuarios que tienen acceso a la base de datos, pero no disponen de una cuenta en la base de datos. No se puede quitar el usuario guest, pero se puede deshabilitar si se revoca su permiso **CONNECT**. El permiso **CONNECT** se puede revocar si se ejecuta **REVOKE CONNECT FROM GUEST** en cualquier base de datos que no sea MASTER ni TEMPDB.

Ejemplo 4

En este ejemplo se verificará el funcionamiento del usuario GUEST.

Crear el inicio de sesión **OPERADOR**:

```
USE master
GO

CREATE LOGIN operador WITH PASSWORD='operador';
GO
```

Ejecute el siguiente script con el inicio de sesión **OPERADOR**:

```
USE EDUTEC
GO
```

Deberías obtener el siguiente mensaje de error:

Msg 916, Level 14, State 1, Line 5
La entidad de seguridad de servidor "operador" no puede tener acceso a la base de datos "EduTec" en el contexto de seguridad actual.

Habilitar el usuario GUEST en la base de datos EDUTEC, este script debes ejecutarlo como inicio de sesión **SA**:

```
USE EDUTEC
GO

GRANT CONNECT TO GUEST
GO

GRANT SELECT ON DBO.PROFESOR TO GUEST
GO
```

Ejecute el siguiente script con el inicio de sesión **OPERADOR**:

```
USE EDUTEC
GO

SELECT USER_NAME(), SUSER_SNAME()
GO

SELECT * FROM DBO.PROFESOR
GO
```

De esta manera se está verificando que el inicio de sesión **OPERADOR** puede acceder a la base de datos **EDUTEC** como usuario **GUEST**.

3 PERMISOS

Todos los elementos protegibles de SQL Server tienen permisos asociados que se pueden conceder a una entidad de seguridad.

3.1 Convenciones de nomenclatura de permisos

A continuación, se describen las convenciones generales que se siguen en la nomenclatura de permisos:

➤ **CONTROL**

Confiere al receptor del permiso capacidades relacionadas con la propiedad. El receptor del permiso dispone de hecho de todos los permisos definidos para el elemento protegible. Una entidad de seguridad a la que se le haya

concedido el permiso CONTROL también puede conceder permisos para el elemento protegible. Como el modelo de seguridad de SQL Server es jerárquico, el permiso CONTROL de un determinado ámbito incluye implícitamente el mismo permiso CONTROL para todos los elementos protegibles que abarca dicho ámbito. Por ejemplo, el permiso CONTROL en una base de datos implica todos los permisos de la base de datos, todos los permisos en todos los ensamblados y todos los esquemas de la misma, así como todos los permisos en los objetos de todos los esquemas que incluye la base de datos.

➤ **ALTER**

Confiere la posibilidad de cambiar las propiedades, excepto la propiedad, de un elemento protegible determinado. Cuando se concede para un ámbito, ALTER también confiere la posibilidad de modificar, crear o quitar cualquier elemento protegible que esté contenido en ese ámbito. Por ejemplo, el permiso ALTER en un esquema incluye la posibilidad de crear, modificar y quitar objetos del esquema.

- **ALTER ANY <Server Securable>**, donde Server Securable puede ser cualquier elemento protegible de servidor.

Confiere la posibilidad de crear, modificar o quitar instancias individuales de Server Securable. Por ejemplo, ALTER ANY LOGIN confiere la posibilidad de crear, modificar o quitar cualquier inicio de sesión en la instancia.

- **ALTER ANY <Database Securable>** donde Database Securable puede ser cualquier elemento protegible en el nivel de base de datos.

Confiere la posibilidad de crear, modificar o quitar instancias individuales de Database Securable. Por ejemplo, ALTER ANY SCHEMA confiere la posibilidad de crear, modificar o quitar cualquier esquema en la base de datos.

➤ **TAKE OWNERSHIP**

Permite al receptor del permiso tomar propiedad del elemento protegible para el que se concede este permiso.

- **IMPERSONATE <Login>**

Permite al receptor suplantar el inicio de sesión.

- **IMPERSONATE <User>**

Permite al receptor suplantar al usuario.

- **CREATE <Server Securable>**

Confiere al receptor la posibilidad de crear Server Securable.

➤ **CREATE <Database Securable>**

Confiere al receptor la posibilidad de crear Database Securable.

➤ **CREATE <Schema-contained Securable>**

Confiere la posibilidad de crear el elemento protegible contenido en el esquema. No obstante, para crear el elemento protegible en un esquema concreto se requiere el permiso ALTER en el esquema.

➤ **VIEW DEFINITION**

Permite al receptor obtener acceso a los metadatos.

➤ **REFERENCES**

El permiso REFERENCES es necesario en una tabla para crear una restricción FOREIGN KEY que hace referencia a esa tabla.

El permiso de REFERENCES es necesario en un objeto para crear FUNCTION o VIEW con la cláusula WITH SCHEMABINDING que hace referencia a ese objeto.

3.2 Permisos aplicables a elementos protegibles específicos

En la siguiente tabla se enumeran los principales tipos de permisos y los tipos de elementos protegibles a los que se pueden aplicar.

PERMISO	SE APLICA A
SELECT	<ul style="list-style-type: none">▪ Sinónimos▪ Tablas y columnas▪ Funciones con valores de tabla, Transact-SQL y Common Language Runtime (CLR), y columnas▪ Vistas y columnas
VIEW CHANGE TRACKING	<ul style="list-style-type: none">▪ Tablas▪ Esquemas
UPDATE	<ul style="list-style-type: none">▪ Sinónimos▪ Tablas y columnas▪ Vistas y columnas▪ Objetos de secuencia

REFERENCES	<ul style="list-style-type: none"> ▪ Funciones escalares y de agregado (Transact-SQL y CLR) ▪ Colas de Service Broker ▪ Tablas y columnas ▪ Funciones con valores de tabla (Transact-SQL y CLR), y columnas ▪ Tipos ▪ Vistas y columnas ▪ Objetos de secuencia
INSERT	<ul style="list-style-type: none"> ▪ Sinónimos ▪ Tablas y columnas ▪ Vistas y columnas
DELETE	<ul style="list-style-type: none"> ▪ Sinónimos ▪ Tablas y columnas ▪ Vistas y columnas

3.3 Directores (Principals)


- Individuos, grupos y procesos que requieren recursos de SQL Server.
- A nivel Windows: grupo Windows, cuenta de usuario de dominio, cuenta de usuario local.
- A nivel SQL Server: login, rol de servidor.
- A nivel base de datos: usuario, rol de base de datos, rol de aplicación, grupo.

3.4 Asegurables (Securables)

- Recursos para los que SQL Server controla el acceso.
- Asegurables con alcance servidor: login, base de datos, TDS endpoint.
- Asegurables con alcance base de datos: usuario, rol de base de datos, rol de aplicación, esquema.
- Asegurables con alcance de esquema: objeto de esquema.

3.5 Permisos

Cada asegurable SQL Server tiene asociado permisos que pueden concederse a un director (principal).

 **Actividad:** Identifique en SQL Server Management Studio los directores, asegurables y permisos.

4 SEGURIDAD A NIVEL DEL SERVIDOR

4.1 Tipos de autenticación

- **Autenticación Windows:** el usuario es autenticado por Windows, y accede a SQL Server mediante un inicio de sesión mapeado a su cuenta de usuario Windows.
- **Autenticación SQL:** el usuario es autenticado por SQL Server mediante su inicio de sesión.


4.2 Modos de autenticación

- **Solo Windows:** el usuario solo puede acceder si tiene un inicio de sesión mapeado a su cuenta Windows.
- **Mixto (SQL y Windows):** si el usuario dispone de una conexión de confianza accede usando autenticación Windows; el usuario con conexión no confiable puede acceder usando autenticación SQL.


 **Actividad:** Verifique cuál es el modo de autenticación usado por su SQL Server.

4.3 Políticas de manejo de contraseñas

Si SQL Server se instala sobre Windows Server 2003 o superior, puede hacer uso de las políticas de manejo de contraseñas de Windows.


 **Actividad:** Busque en los Libros en Pantalla de SQL Server, información sobre las políticas de manejo de contraseñas.

4.4 Creación de un inicio de sesión

 **Actividad:** Desde SQL Server Management Studio cree un inicio de sesión identificado con su nombre y apellido, y que tenga acceso a las bases de datos **Northwind** y **EduTec**, donde Northwind es la base de datos predeterminada.


4.5 Rol fijo de servidor

Reúne un conjunto de permisos para ejecutar cierto tipo de tareas administrativas sobre el servidor.

 **Actividad:** Identifique en SQL Server Management Studio los roles fijos de servidor.

4.6 Suplantación o Delegación


Permite que una instancia de SQL Server se conecte a otra instancia SQL Server bajo el contexto de un usuario autenticado Windows para, por ejemplo, ejecutar consultas distribuidas.

 **Actividad:** Buscar en los Libros en Pantalla de SQL Server, información acerca de los requisitos para especificar delegación. Si le es posible, ejecute una práctica con el escenario descrito en el artículo correspondiente de los Libros en Pantalla.

4.7 Credenciales

- Representación alternativa de un login.
- Permite que un usuario conectado a SQL Server acceda a recursos fuera de SQL Server.
- Generalmente consisten del usuario Windows y su contraseña.

4.8 Concesión de permisos

 **Actividad:** Identificar consultando los Libros en Pantalla, los permisos que se pueden aplicar a diferentes asegurables.

5 SEGURIDAD A NIVEL DE LA BASE DE DATOS

5.1 Usuarios


- Un usuario permite ejecutar tareas sobre la base de datos, ya que es el usuario quien obtiene los permisos.
- Un usuario se puede mapear a un login o a un grupo Windows.

5.2 Usuario DBO

- Es el usuario reconocido como dueño de la base de datos.
- Cada base de datos tiene su usuario dbo.
- Los miembros del rol sysadmin y el inicio de sesión SA son mapeados al usuario dbo.
- Cualquier objeto creado por un miembro de sysadmin pertenece al dbo.
- El usuario dbo no puede ser eliminado.


5.3 Usuario GUEST

- Cada base de datos tiene su usuario guest.
- Por defecto, el usuario está deshabilitado.
- Permite que los logins que no tienen usuario mapeado accedan a la base de datos.

 **Actividad:** Identifique a los usuarios dbo y guest de la base de datos Northwind.


5.4 Rol de base de datos

Reúne un conjunto de permisos para ejecutar cierto tipo de tareas administrativas sobre la base de datos.

 **Actividad:** Identifique en SQL Server Management Studio los roles de base de datos en Northwind.


5.5 El rol de base de datos Public

- Agrupa a todos los usuarios de la base de datos.
- Permite establecer los permisos mínimos comunes para todos los usuarios.

 **Actividad:** Defina que los miembros del rol Public solo pueden leer la Lista de Precios de Northwind.

5.6 Rol de Aplicación

Permite que una aplicación se ejecute con su propio conjunto de privilegios.

 **Actividad:** Averiguar en los Libros en Pantalla de SQL Server, el procedimiento para definir y aplicar un rol de aplicación.

6 CURSOS RELACIONADOS

<https://www.ceps.uni.edu.pe/>



