Seguridad en Bases de Datos

Tema

6

# Autenticación y Seguridad en SQL Server

Universidad Francisco de Vitoria
UFV Madrid

*Grado en Ingeniería Informática*
*Escuela Politécnica Superior*

# Objetivos y resultados de aprendizaje

Una parte importante del trabajo de un administrador de bases de datos consiste en planear y crear bases de datos.

Un aspecto importante de esa planificación se centra en el establecimiento de un entorno de seguridad que permita cumplir con los criterios de Accesibilidad, Confidencialidad e Integridad.

**Objetivo:**

- Manejar los principios de seguridad que influyen en la seguridad de una BBDD y del sistema en que se ubica.

# Evaluación del tema

Los resultados de aprendizaje correspondiente a este tema se evaluarán con los siguientes tipos de pruebas:

- Pruebas escritas de carácter teórico-práctico
- Entrega de Prácticas
- Participación en clase

# Bibliografía

Para obtener más información puedes consultar:


- Libros en pantalla de SQL Server.
- STANEK, WILLIAM R. SQL Server 2012 Guía del Administrador. Editorial Anaya. Madrid 2013. ISBN 84-4153221-2.

# Índice de contenidos

# Introducción

El principal problema que se nos presenta a la hora de proteger cualquier sistema informático, es asegurar la confiabilidad del mismo (Impedir el acceso no autorizado).

El objetivo habitual para cualquier atacante es obtener la información contenida en el sistema. En el caso de las bases de datos empresariales, estas contienen los datos de negocio y gestión de la misma. Ello implica que son el objetivos prioritarios de los atacantes.

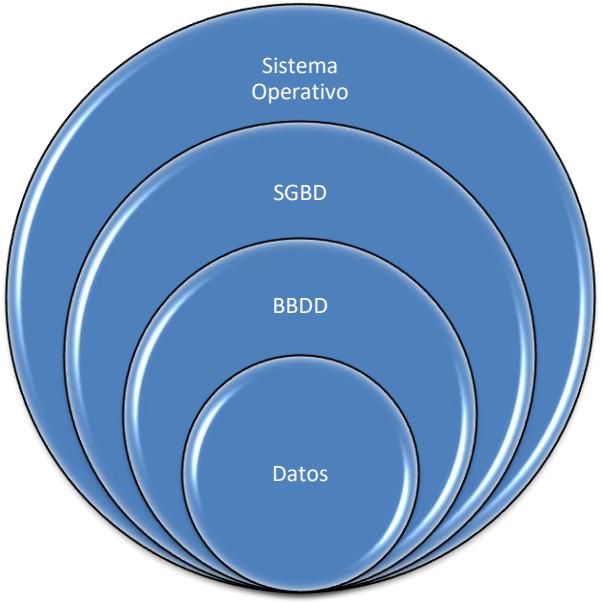
Su protección implica por tanto, la protección de la organización y se constituye en un pilar del funcionamiento empresarial.

No se debe olvidar además las repercusiones legales y reputacionales que la empresa puede sufrir si sus datos son divulgados. Aspecto este muy en boga actualmente (RRSS).

# Introducción

Parece importante recordar que nuestras BBDD no son en modo alguno elementos independientes y aislados del resto de sistema de información. Es por ello que nuestra primera tarea ha de consistir en la correcta ubicación del activo y el posterior estudio de las necesidades de protección del mismo.

El ecosistema del Servidor de datos es el objeto de estudio de la presente asignatura.




Además de proteger el servidor de datos también es importante la securización de otros ámbitos del sistema información:

- Red
- Físico
- Humano

# Introducción

Hemos comentado anteriormente que el acceso a los datos con intención de ser divulgados o usados es el más habitual de los objetivos de los atacantes. Aún así también es común ataques que pretenden la modificación no autorizada de los datos (Integridad) o la destrucción de estos (Disponibilidad).

Para impedir estas acciones debemos trabajar diversos aspectos que impidan la materialización de los ataques mediante la reducción o eliminación de las vulnerabilidades de nuestro sistema de información:

- Restricción de los niveles de acceso (privilegios) a los distintos Usuarios
- Estratificación de los datos
- Codificación de los datos y comunicaciones

# Modelos de Autenticación

Universidad Francisco de Vitoria UFV Madrid

Las Credenciales (Usuario + Password) se usan para:

- Permitir que alguien inicie la sesión en un equipo basándose en la identidad de la cuenta de usuario.
- Permitir que los procesos y servicios se ejecuten dentro de un contexto de seguridad específico.
- Administrar el acceso de un usuario a los recursos

Entidad de Seguridad

- Una entidad de seguridad es cualquier identidad autenticada a la que se puede conceder permiso para tener acceso a un objeto del sistema de base de datos.
- Se puede distinguir entre entidades principales indivisibles y entidades de seguridad de colección.
- Pueden existir en diversos niveles, dependiendo cual es el servicio que verifica sus credenciales.

# Modelos de Autenticación

Universidad Francisco de Vitoria UFV Madrid

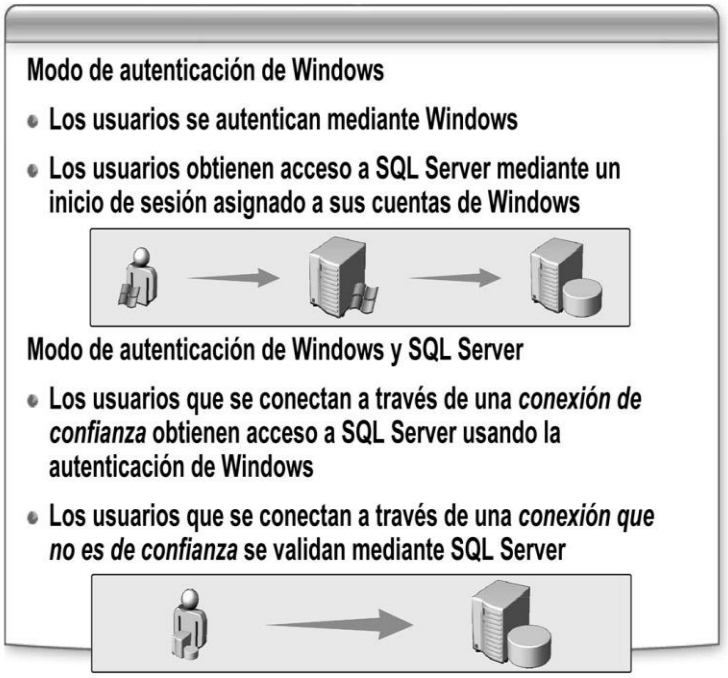
Por defecto, en SQL Server encontraremos dos modos de autenticación:

- Modo Windows: el modo Windows permite conectar con la base de datos usando credenciales de Windows (por ejemplo, conectando con un usuario de dominio).
- Modo Mixto: el modo mixto permite, además de la anterior, autenticar usando credenciales definidas en el propio SQL. De esta manera, se podrán crear usuarios en el SQL Server, que sin necesidad de existir en el dominio, permitan el acceso a la base de datos.
- Durante una instalación de SQL Server, se podrá escoger el tipo de autenticación que se quiere usar.

# Modelos de Autenticación

Universidad Francisco de Vitoria UFV Madrid

Las necesidades de seguridad del entorno del servidor y de red determinarán el modo de autenticación que se usará para acceder a la BBDD




La autenticación de Windows proporciona varias ventajas sobre la autenticación de SQL Server:

- Le permite agregar grupos de usuarios a SQL Server mediante la agregación de una cuenta de inicio de sesión única.
- Permite a los usuarios un rápido acceso a SQL Server sin tener que recordar otra cuenta de inicio de sesión y contraseña.

# Modelos de Autenticación

Universidad Francisco de Vitoria UFV Madrid

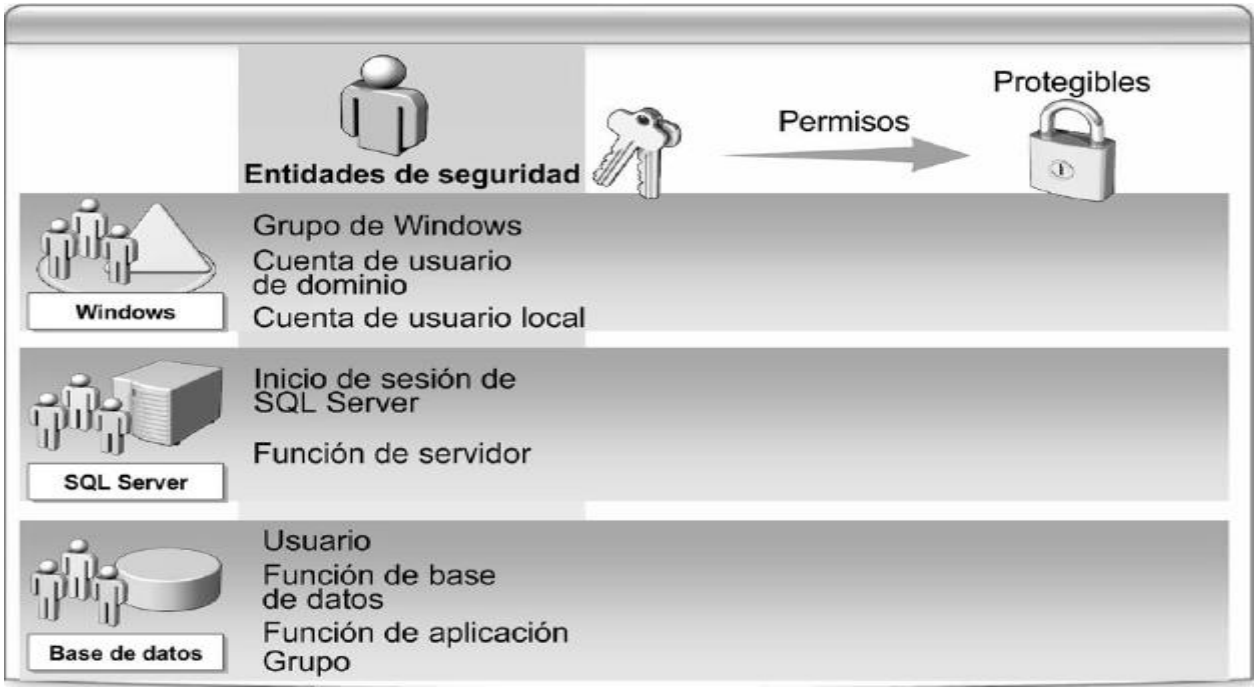
Usar autenticación SQL Server cuando se deba permitir que se conecten usuarios o aplicaciones que no tienen las credenciales de Windows.

Autenticación de Windows vs Autenticación SQL Server

- La autenticación de Windows no exige que los nombres de usuario y las contraseñas pasen por la red al conectarse a SQL Server. En su lugar, se usa el símbolo de acceso de usuario de Windows, lo que hace más segura la autenticación de Windows.
- La autenticación de Windows requiere menos sobrecarga administrativa, ya que el acceso a SQL Server puede lograrse mediante un inicio de sesión que se asigna a un grupo de Windows, y la administración de cada uno de los usuarios se confina al dominio de Windows.
- El modo de autenticación SQL Server aumenta la superficie del sistema de SQL Server, lo que lo hace más vulnerable ante cualquier ataque.

# Implementación

Una **entidad de seguridad** es cualquier identidad autenticada a la que se puede conceder permiso para tener acceso a un objeto del sistema de base de datos. SQL Server distingue entre entidades principales indivisibles, que son identidades únicas (como, por ejemplo, inicios de sesión), y entidades de seguridad de colección, que son colecciones de identidades (tales como funciones fijas de servidor).



# Implementación

Universidad Francisco de Vitoria UFV Madrid

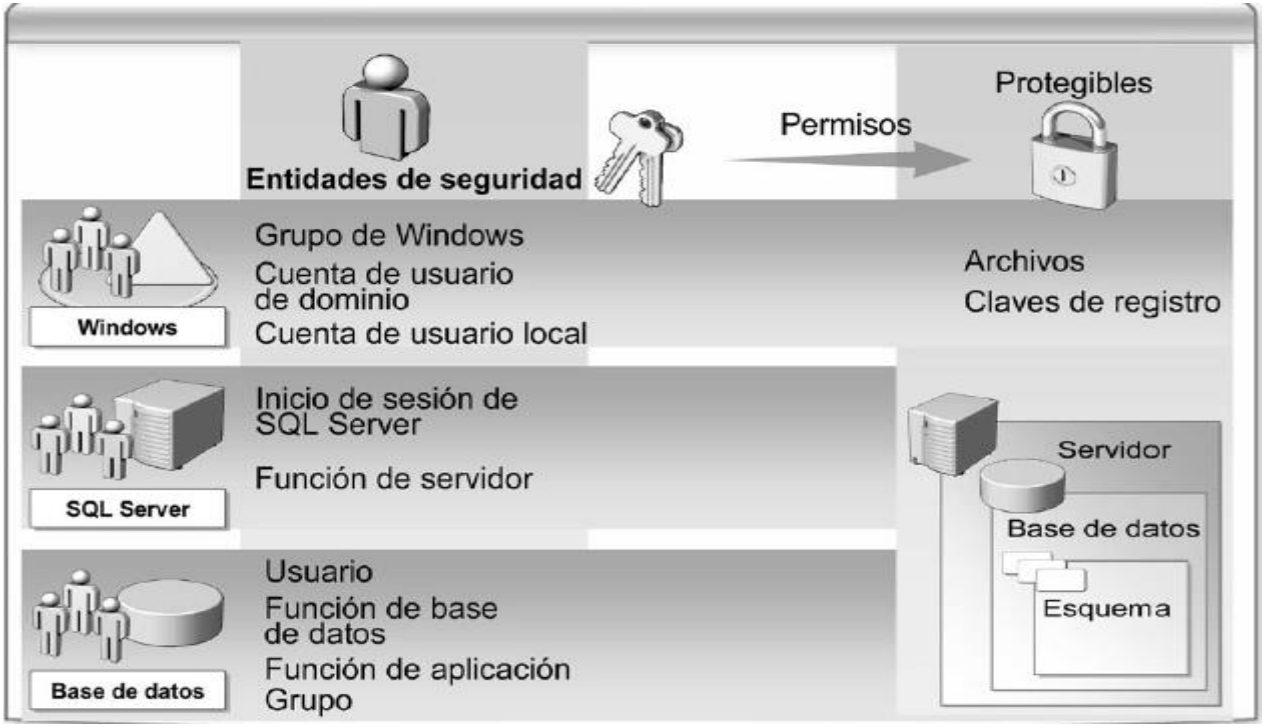
Las entidades de seguridad existen en tres niveles: Microsoft Windows®, SQL Server y base de datos. Los tipos de entidad de seguridad posibles en cada uno de estos niveles se muestran en la tabla siguiente.

| Nivel | Entidades de Seguridad |
|---|---|
| Windows | Cuenta de usuario local de Windows<br>Cuenta de usuario de dominio de Windows<br>Grupo de Windows |
| SGBD (SQL Server) | Inicio de sesión de SQL Server<br>Función de SQL Server |
| Base de Datos | Usuario de la base de datos<br>Función de la base de datos<br>Función de aplicación |

# Implementación

Universidad Francisco de Vitoria UFV Madrid

Los objetos cuyo acceso está regulado por el sistema de autorización de SQL Server se denominan **protegibles**. Los protegibles se organizan en jerarquías anidadas llamadas ámbitos, que también se pueden proteger.



# Implementación

Universidad Francisco de Vitoria UFV Madrid

| Ámbito | Protegibles |
|---|---|
| de Servidor | ■ Inicios de sesión<br>■ Extremos<br>■ Bases de datos |
| De Base de Datos | ■ Usuarios<br>■ Funciones<br>■ Funciones de aplicación<br>■ Certificados<br>■ Claves simétricas<br>■ Claves asimétricas<br>■ Ensamblados<br>■ Catálogos de texto completo<br>■ Eventos DDL<br>■ Esquemas |
| De Esquema | ■ Tablas<br>■ Vistas<br>■ Funciones<br>■ Procedimientos<br>■ Tipos<br>■ Sinónimos<br>■ Agregados |

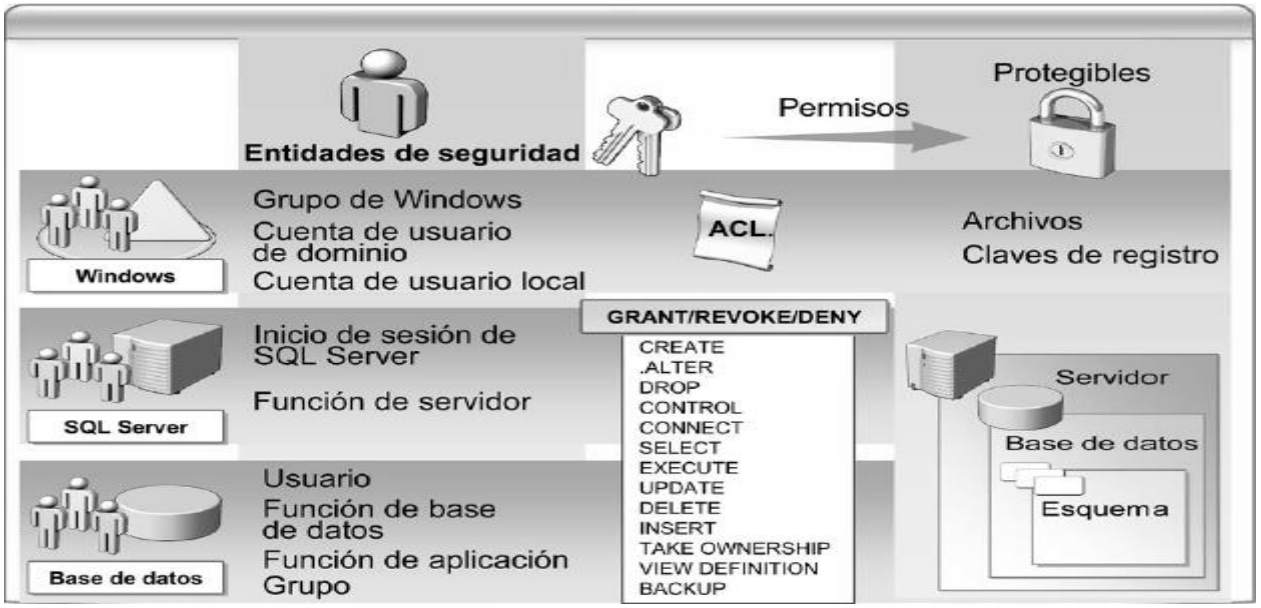
Los tres ámbitos protegibles son servidor, base de datos y esquema. Los protegibles en el nivel de Windows incluyen archivos y claves del Registro.

Una entidad de seguridad también puede ser un protegible. Por ejemplo, un inicio de sesión es una entidad de seguridad, pero también se pueden otorgar permisos en ese inicio de sesión a otros inicios de sesión, lo que lo convierte en un protegible.

# Implementación

SQL Server usa **permisos** para controlar el acceso a los protegibles por parte de entidades de seguridad.

Los permisos son las reglas que gobiernan el nivel de acceso de las entidades de seguridad a los protegibles. Se pueden otorgar, revocar o denegar permisos en un sistema de SQL Server. Todos los protegibles de SQL Server tienen permisos asociados que pueden otorgarse a cada entidad de seguridad.



# Implementación

Universidad Francisco de Vitoria UFV Madrid

Determinados permisos en SQL Server 2005 se pueden heredar a través de un permiso concedido en un nivel más alto de la jerarquía de ámbito del protegible. Por ejemplo:

- Una entidad de seguridad a la que se le ha concedido el permiso SELECT en un esquema hereda automáticamente el permiso SELECT en todos los objetos del esquema.
- Una entidad de seguridad a la que se la ha concedido el permiso CONTROL en un objeto de base de datos hereda automáticamente el permiso CONTROL en todos los protegibles que contiene esa base de datos y todos los protegibles que contienen los esquemas incluidos en esa base de datos.

Una entidad de seguridad puede realizar una acción determinada (Permisos efectivos) si:

- El permiso se ha concedido explícitamente a la entidad de seguridad o a una colección de la que es miembro la entidad de seguridad, y…
- El permiso no se ha denegado explícitamente a la entidad de seguridad o a una colección de la que es miembro la entidad de seguridad.

# Auditoría

Universidad Francisco de Vitoria UFV Madrid

Auditar todo el sistema es en la mayoría de los caos imposible, ya que supondría un alto coste y se obtendría un elevado volumen de datos que harían difícil sus análisis.

Lista de Control de Acceso al Sistema (SACL)

- Los Usuarios o grupos que se auditan al acceder al recurso
- Recursos sobre los que se establece la auditoria aplicar
- Eventos auditables

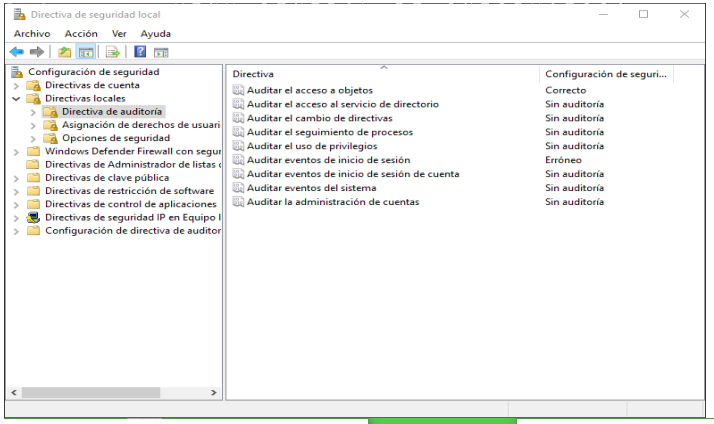
Los valores posible al establecer una auditoria son por lo general:

- Correcto: Se registran todos los suceso correctos
- Error: Se registran los suceso erróneos

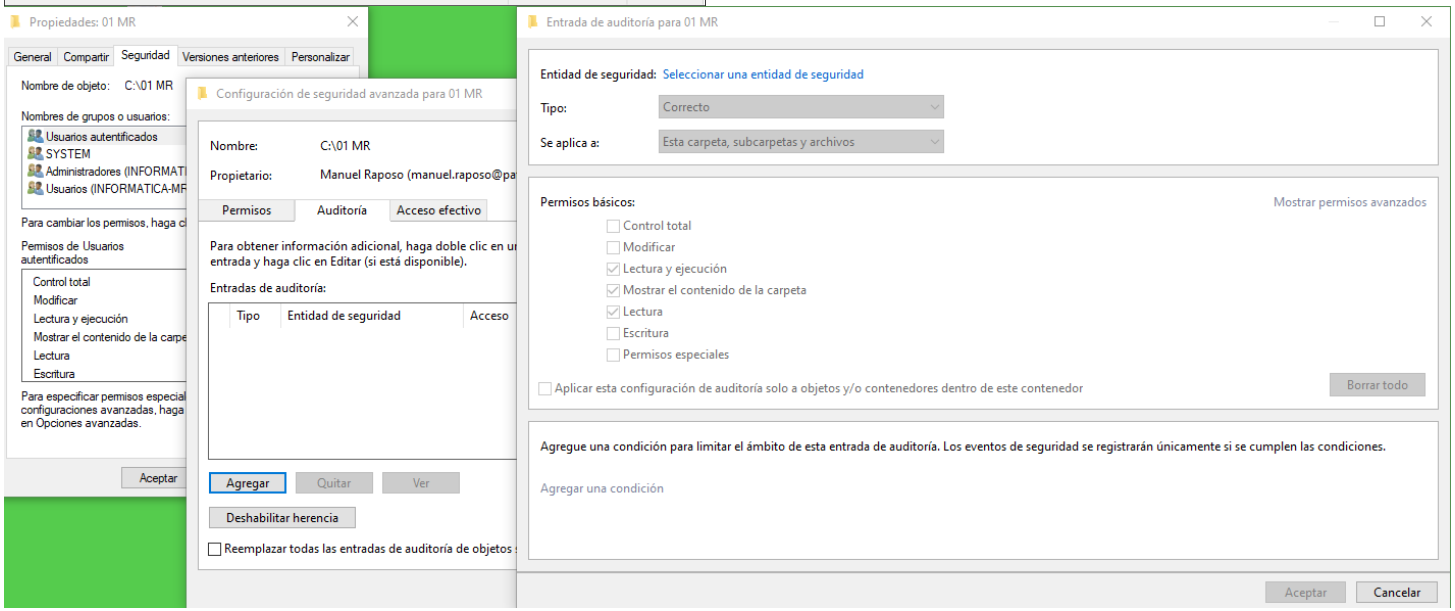
# Auditoría

Universidad Francisco de Vitoria UFV Madrid

Auditar un Fichero o Carpeta.




- Debemos activar la directiva de Auditoria correspondiente y posteriormente…
- …Establecer el valor de auditoria en el objeto deseado (Fichero /Carpeta)



# Auditoría

Universidad Francisco de Vitoria UFV Madrid

Auditar el SGBD

- La auditoría de una instancia del SGBD implica el seguimiento y registro de los eventos que se producen en Motor de base de datos.
- Los eventos auditados se pueden escribir en los registros de eventos o en los archivos de auditoría.
- Puede registrar grupos de acciones de auditoría en el servidor por instancia, así como grupos de acciones o acciones de auditoría en la base de datos por base de datos.
- El evento de auditoría se producirá cada vez que se encuentre la acción auditable.

- https://docs.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-database-engine?view=sql-server-ver15

# Auditoría

Universidad Francisco de Vitoria UFV Madrid

Auditar el Servidor

- La especificación de auditoría de servidor recopila muchos grupos de acciones de nivel de servidor generados por la característica Extended Events.
- Puede incluir grupos de acciones de auditoría en una especificación de auditoría de servidor.
- Los grupos de acciones de auditoría son grupos predefinidos de acciones, que constituyen eventos atómicos que tienen lugar en el Motor de base de datos.
- Estas acciones se envían a la auditoría, que las registra en el destino.

- https://docs.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15

# Auditoría

Universidad Francisco de Vitoria UFV Madrid

Auditar la Base de Datos

- La especificación de auditoría de base de datos recopila acciones de auditoría de nivel de base de datos generadas por la característica Extended Events.
- Puede agregar grupos de acciones de auditoría o eventos de auditoría a una especificación de auditoría de base de datos.
- Los eventos de auditoría son las acciones atómicas que puede auditar el motor de SQL Server .
- Los grupos de acciones de auditoría son grupos predefinidos de acciones. Ambos están en el ámbito de la base de datos de SQL Server.
- Estas acciones se envían a la auditoría, que las registra en el destino.

- https://docs.microsoft.com/es-es/sql/relational-databases/security/auditing/sql-server-audit-action-groups-and-actions?view=sql-server-ver15